PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-094552

(43)Date of publication of application : 06.04.2001

(51)Int.Cl. H04L 9/18
G06F 12/14
H04L 9/08

(21)Application number : 11-267262

(22)Date of filing : 21.09.1999

(71)Applicant : SONY CORP

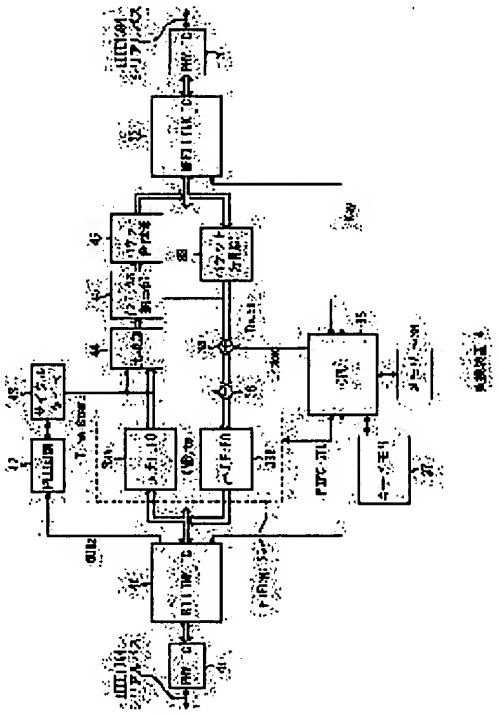
(72)Inventor : MORINAGA TAKEO

(54) DEVICE AND METHOD FOR DATA PROCESSING AND RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To protect digital contents from illegal copying and to record the contents with a DVCR, which does not meet the standards of DTCP (Digital Transmission Content Protection).

SOLUTION: A converting device 4 which meets the standards of DTCP extracts a key used for ciphering and deciphering from a ciphered TS packet from a digital CS tuner by an MPEG link IC 32, and a CPU 35 stores the key to a key memory 37 while relating the key to an index for specifying it. Further, a packet division part 33 converts the ciphered TS packet into a DIF block which can be recorded by a DVCR and a computing element 34 adds the index made to correspond to the key at the position where the key is included in the DIF block. The resulting DIF block is outputted to an external DVCR and recorded.



LEGAL STATUS

[Date of request for examination] 01.03.2006

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than

the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

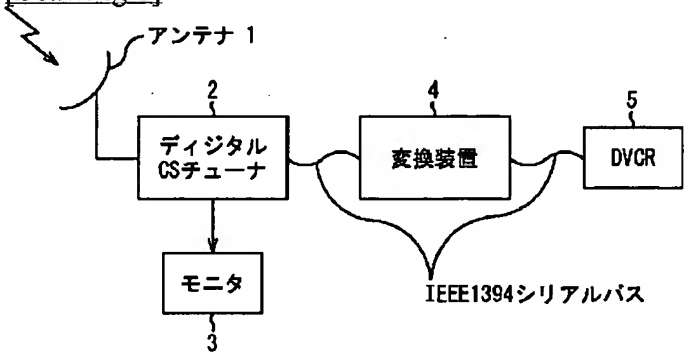
* NOTICES *

JPO and INPIT are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

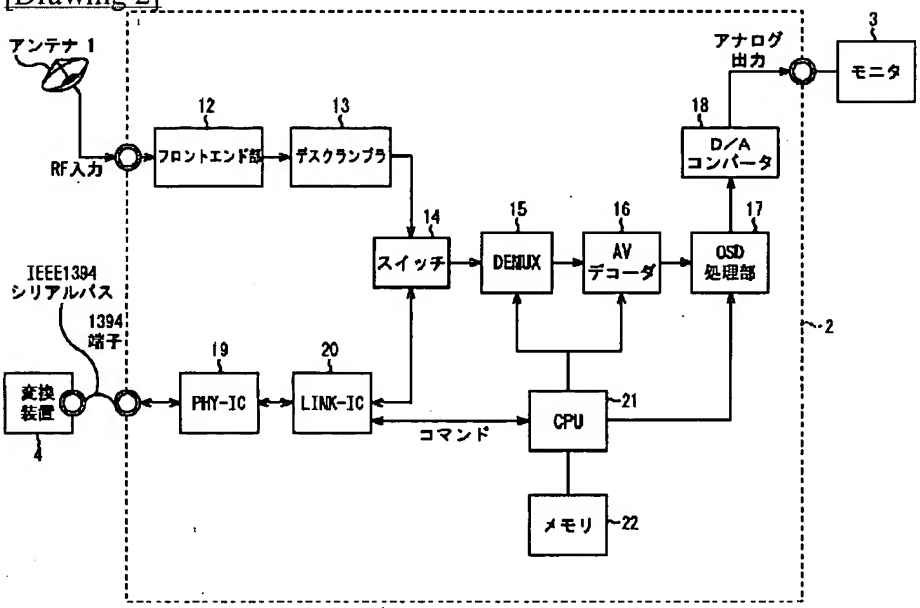
DRAWINGS

[Drawing 1]

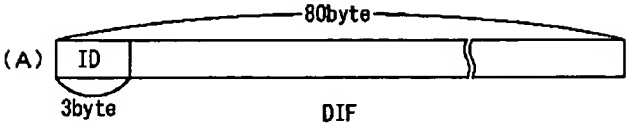


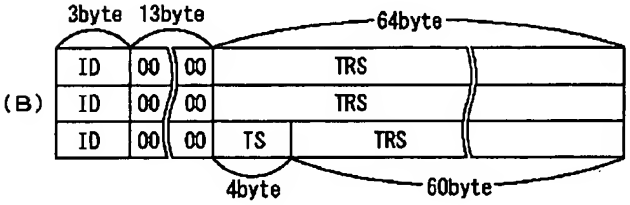
ディジタル衛星放送受信システム

[Drawing 2]

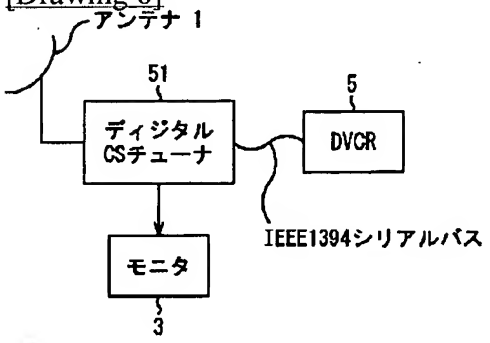


[Drawing 4]



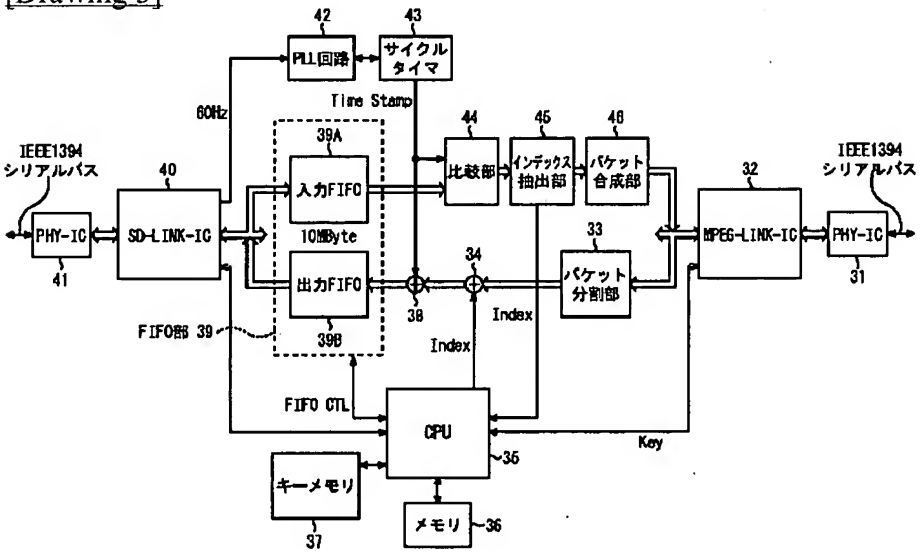


[Drawing 8]



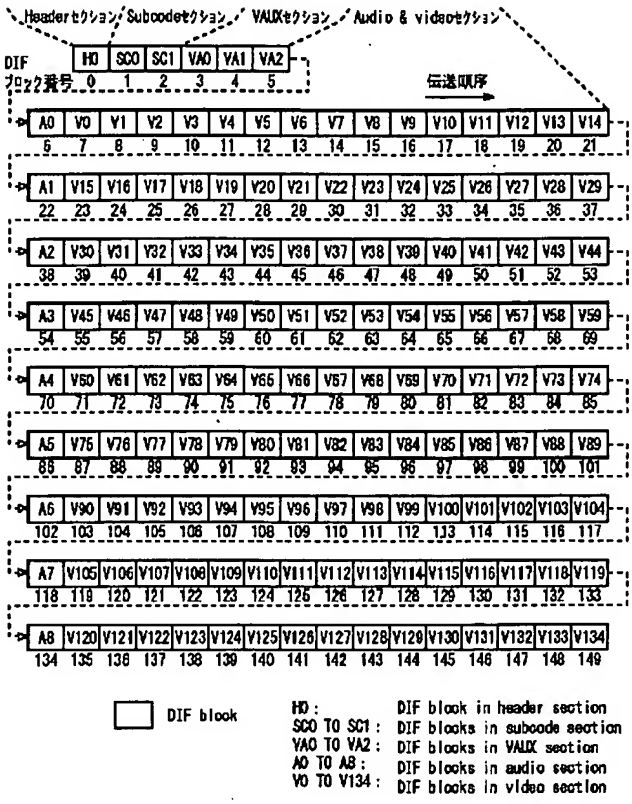
ディジタル衛星放送受信システム

[Drawing 3]



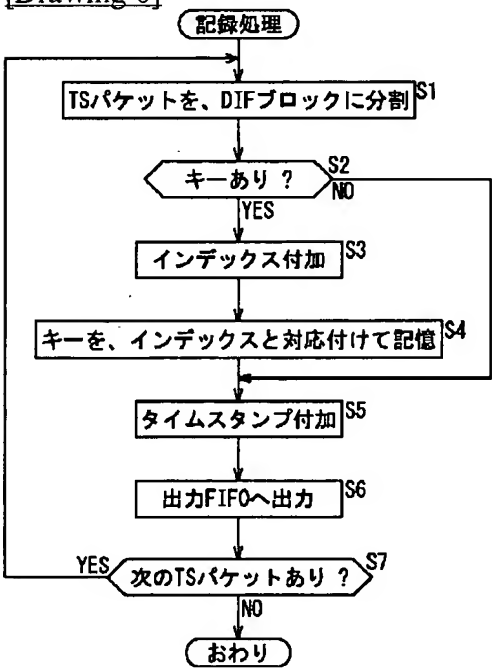
変換装置 4

[Drawing 5]

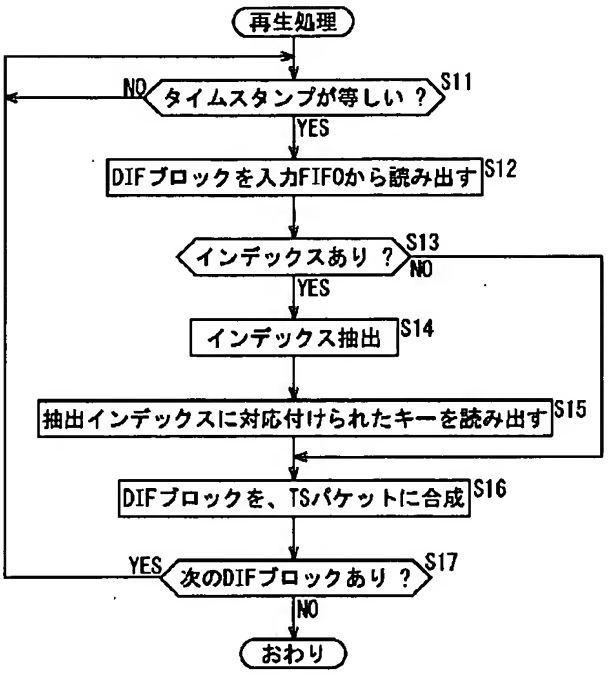


Transmission order of DIF blocks in a DIF sequence

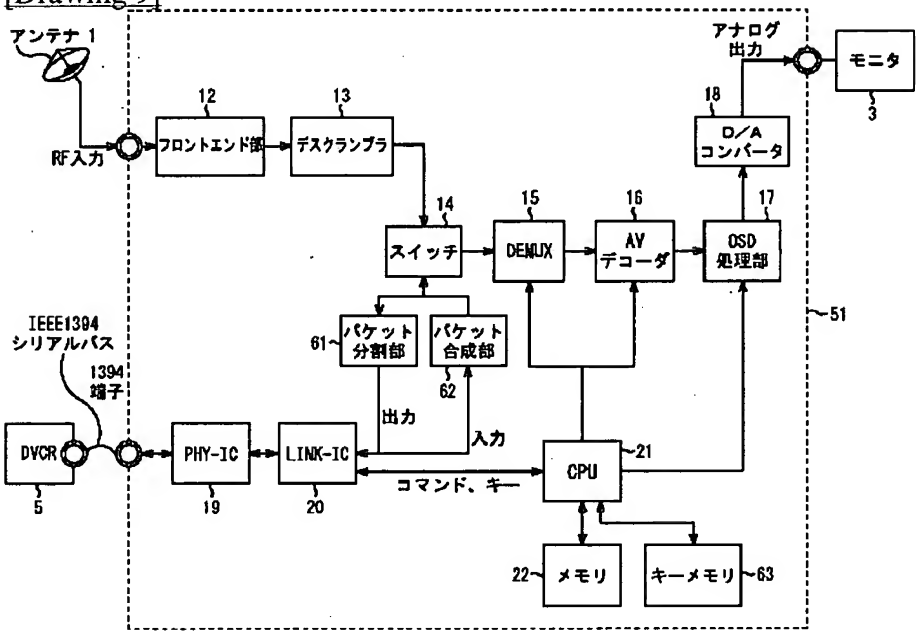
[Drawing 6]



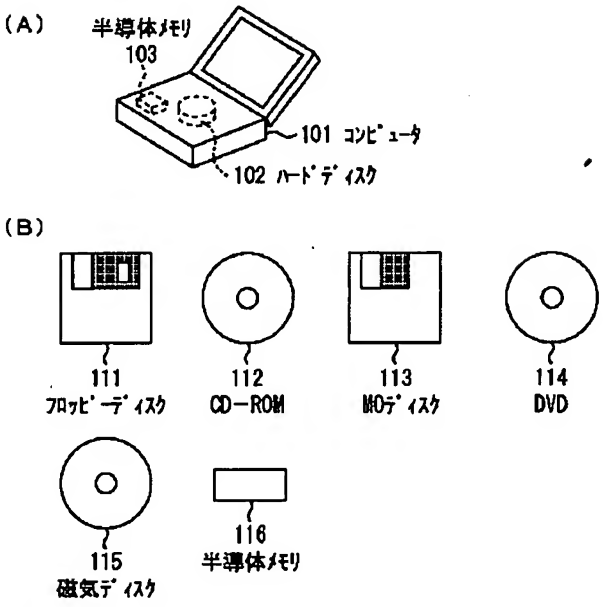
[Drawing 7]



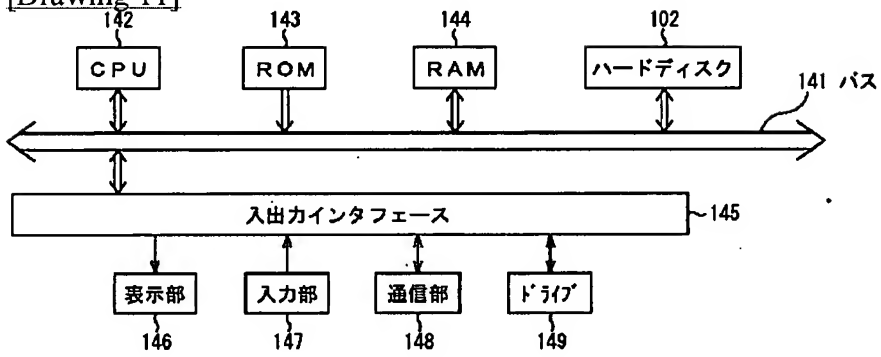
[Drawing 9]



[Drawing 10]



[Drawing 11]



コンピュータ 101

[Translation done.]

* NOTICES *

JPO and INPIT are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] It is the block diagram showing the example of a configuration of the gestalt of 1 operation of the digital satellite broadcasting service receiving system which applied this invention.
[Drawing 2] It is the block diagram showing the example of a configuration of the digital CS tuner 2 of drawing 1 .
[Drawing 3] It is the block diagram showing the example of a configuration of the inverter 4 of drawing 1 .
[Drawing 4] It is drawing for explaining processing of the packet division section 33 of drawing 3 .
[Drawing 5] It is drawing for explaining processing of the computing element 34 of drawing 3 .
[Drawing 6] It is a flow chart for explaining processing of the inverter 4 of drawing 3 in the case of recording by DVCR5.
[Drawing 7] It is a flow chart for explaining processing of the inverter 4 of drawing 3 in the case of reproducing by DVCR5.
[Drawing 8] It is the block diagram showing the example of a configuration of the gestalt of other operations of the digital satellite broadcasting service receiving system which applied this invention.
[Drawing 9] It is the block diagram showing the example of a configuration of the digital CS tuner 51 of drawing 8 .
[Drawing 10] It is drawing for explaining the record medium which applied this invention.
[Drawing 11] It is the block diagram showing the example of a configuration of the computer 101 of drawing 10 .
[Description of Notations]
1 Antenna 2 Digital CS Tuner, 3 Monitor 4 Inverter 5 DVCR 12 The front end section, 13 A descrambler, 14 A switch, 15 DEMUX 16 AV decoder, 17 OSD processing section 18 A D/A converter, 19 FAI IC 20 Link IC 21 CPU 22 Memory, 31 FAI IC 32 The MPEG link IC 33 Packet division section 34 A computing element, 35 CPU 36 memory 37 key memory 38 computing elements 39 The FIFO section The 39A input FIFO 39B Output FIFO 40 The SD link IC 41 FAI IC 42 A PLL circuit, 43 Cycle timer 44 A comparator, 45 The index extract section, 46 The packet composition section, 51 Digital CS tuner 61 packet division section, 62 The packet composition section, 63 A key memory and 101 A computer, 102 Hard disk 103 semiconductor memory, 111 A floppy disk, 112 CD-ROM, 113 An MO disk, 114 DVD 115 Magnetic disk 116 Semiconductor memory 121 download site 122 Satellite 131 A network, 141 Bus 142 CPU 143 ROM 144 RAM 145 Input/output interface 146 Display 147 Input section 148 Communications department 149 drives

---

[Translation done.]

* NOTICES *

JPO and INPIT are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention transmits digital contents to a data processor and the data-processing approach, and a list through an IEEE1394 serial bus etc. especially about a record medium, and relates to a record medium at the data processor and the data-processing approach a substandard recording apparatus also enables it to perform the record, and a list.
[0002]
[Description of the Prior Art] For example, since it can perform an isochronous (isochronous) transfer of data, the communication link by IEEE(Institute of Electrical and Electronics Engineers) 1394 specification which is one of the serial bus specification is suitable for the transfer of digital data with the need of reproducing on real time, such as an image and voice, further, also has the request of the multimedia communication in recent years, and attracts attention greatly.
[0003] By the way, since digital contents, such as a digital video data and digital audio data, can be copied repeatedly, without degrading the image quality and tone quality, they need to protect the copyright person etc. from an illegal copy.
[0004] Then, 5CDTCP (Five Company Digital Transmission Content Protection) (suitably henceforth DTCP) was defined by five companies including Sony Corp. which is this applicant as specification for protecting the digital contents when transmitting digital contents among the equipments connected through the IEEE1394 serial bus.
[0005] In DTCP, in advance of transmission of the digital contents which are not copy free-lancers, a receiving side attests mutually whether the copy control information for controlling a copy can be dealt with correctly, enciphers and transmits digital contents to it in a transmitting side after that, and decodes the enciphered digital contents in a receiving side.
[0006] Encryption of the digital contents by DTCP generates the key which carries out time amount change, and is performed using the key. The enciphered digital contents are transmitted in IEEE1394 serial bus tops including the key used for the encryption, and the enciphered digital contents are decoded in a receiving side using the key contained there.
[0007] Here, according to DTCP, the flag with which the modification timing of the key used for the initial value of a key and encryption of digital contents is expressed to accuracy is included in the enciphered digital contents (suitably henceforth encryption contents). And at a receiving side, by changing too the initial value of the key contained in the encryption contents to the timing of the flag contained in the encryption contents, the key used for encryption is generated and encryption contents are decoded. In addition, if the key for performing the decode to encryption contents is contained in this description, even if it will think that it is equivalent, in order not to interfere, below, it shall think such.
[0008]
[Problem(s) to be Solved by the Invention] As mentioned above, for example, the digital contents which received with the digital CS (Communication Satellite) tuner are unrecordable through an IEEE1394 serial bus by substandard DVCR (Digital Video Tape Recoder) which cannot deal with copy control

information correctly.
[0009] However, it is expected that the needs to a utilization gestalt which transmits the digital contents which received with the digital CS tuner to DVCR, and records them on videotape through an IEEE1394 serial bus increase from now on.
[0010] Moreover, although digital contents can be protected from an illegal copy if the encryption contents which a digital CS tuner outputs are recorded on videotape as it is by DVCR, it cannot view and listen to the encryption contents recorded on videotape. That is, in the former, it was difficult to reproduce the encryption contents recorded by DVCR, to input into a digital CS tuner, and to perform the decode.
[0011] This invention can be made to perform recording by substandard DVCR etc. while it is made in view of such a situation and protects digital contents from an illegal copy.
[0012]
[Means for Solving the Problem] A key extract means to extract the key by which the data processor of this invention is contained in encryption data, A storage means to match a key with the index for specifying it, and to memorize it, The 1st format conversion means which changes encryption data into the data of a predetermined format, An index addition means to add the index matched with the key to the location where the key of the data of a predetermined format was contained, The 1st output means which outputs outside the data of a predetermined format with which the index was added, An index extract means to extract an index from the data of the predetermined format supplied from the outside, The 2nd format conversion means which changes the data of a predetermined format into the encryption data of the original format, It is characterized by including a key addition means to add the key matched with the index to the location where the index of encryption data was contained, and the 2nd output means which outputs outside the encryption data with which the key was added.
[0013] Encryption data can be made into a transport stream.
[0014] The data of a predetermined format can be used as the data of a DIF (Digital Interface) format.
[0015] The specification of the equipment which receives the data of a predetermined format by which encryption data were connected to whether a copy is permitted and or not the exterior can be made to restrict the output of the data of a predetermined format to the 1st output means. Moreover, the 1st output means can be made to operate the copy control information for controlling the copy about the data when outputting the data of a predetermined format.
[0016] The key extract step which extracts the key by which the data-processing approach of this invention is included in encryption data, The storage step which matches a key with the index for specifying it, and memorizes it, The 1st format conversion step which changes encryption data into the data of a predetermined format, The index addition step which adds the index matched with the key to the location where the key of the data of a predetermined format was contained, The 1st output step which outputs outside the data of a predetermined format with which the index was added, The index extract step which extracts an index from the data of the predetermined format supplied from the outside, The 2nd format conversion step which changes the data of a predetermined format into the encryption data of the original format, It is characterized by including the key addition step which adds the key matched with the index to the location where the index of encryption data was contained, and the 2nd output step which outputs outside the encryption data with which the key was added.
[0017] The key extract step which extracts the key by which the record medium of this invention is contained in encryption data, The storage step which matches a key with the index for specifying it, and memorizes it, The 1st format conversion step which changes encryption data into the data of a predetermined format, The index addition step which adds the index matched with the key to the location where the key of the data of a predetermined format was contained, The 1st output step which outputs outside the data of a predetermined format with which the index was added, The index extract step which extracts an index from the data of the predetermined format supplied from the outside, The 2nd format conversion step which changes the data of a predetermined format into the encryption data of the original format, It is characterized by recording the program containing the key addition step which adds the key matched with the index to the location where the index of encryption data was contained,

and the 2nd output step which outputs outside the encryption data with which the key was added.
[0018] The key contained in encryption data in the record medium at the data processor of this invention and the data-processing approach, and the list is extracted, and the key matches with the index for specifying it, and is memorized. Furthermore, encryption data are changed into the data of a predetermined format, and the index matched with the key is added to the location where the key of the data of the predetermined format was contained, and it is outputted to it outside. On the other hand, an index is extracted and the data of the predetermined format are changed into the encryption data of the original format from the data of the predetermined format supplied from the outside. And the key matched with the index is added to the location where the index of encryption data was contained, and it is outputted to it outside.
[0019]
[Embodiment of the Invention] Drawing 1 shows the example of a configuration of the gestalt of 1 operation of the digital satellite broadcasting service receiving system which applied this invention.
[0020] It is received by the antenna 1 and the digital satellite broadcast wave broadcast from digital Satellite Broadcasters which does not illustrate is supplied to the digital CS tuner 2. The digital CS tuner 2 has a specification based on DTCP, from the signal supplied from an antenna 1, it detects the input signal of a predetermined frequency band, gets over, and makes it an MPEG (Moving Picture Experts Group) transport stream. Furthermore, in the digital CS tuner 2, the thing of one predetermined channel is extracted among TS packets (Transport Stream packet) which constitute the transport stream, and MPEG 2 decoding of the video data and audio data which are contained in the extracted TS packet and by which MPEG 2 encoding was carried out is carried out. And the video data or audio data obtained as a result of the decoding is supplied to a monitor 3, and is outputted as a display or voice as an image, respectively.
[0021] Moreover, in the digital CS tuner 2, from a transport stream, TS packet of one or more channels is extracted, and it is enciphered by the method based on DTCP. And the enciphered TS packet (following, suitably encryption TS packet) is supplied to an inverter 4 through an IEEE1394 serial bus.
[0022] Here, an inverter 4 performs the communication link based on DTCP, when exchanging digital contents between the digital CS tuners 2 through an IEEE1394 serial bus. Therefore, all, after the digital CS tuner 2 and an inverter 4 perform mutual recognition, using the key which carries out time amount change, they encipher digital contents and output them to the encryption contents obtained as a result on an IEEE1394 serial bus including the key used for encryption.
[0023] In an inverter 4, format conversion of the encryption TS packet from the digital CS tuner 2 is carried out to the DIF (Digital Interface) block of SD (Standard density) specification, and it is supplied to DVCR5 through an IEEE1394 serial bus. In DVCR5 which is DV (Digital Video) device, the DIF block from an inverter 4 is recorded on the digital video tape which is not illustrated.
[0024] Here, about the DIF format, the detail is indicated by Specification of Consumer Use Digital VCRs summarized in HD Digital VCR Conference, for example.
[0025] Furthermore, in DVCR5, the DIF block recorded on the digital video tape is reproduced, and an inverter 4 is supplied through an IEEE1394 serial bus. In an inverter 4, format conversion of the DIF block from DVCR5 is carried out to the original encryption TS packet, and it is supplied to the digital CS tuner 2 through an IEEE1394 serial bus. In the digital CS tuner 2, the encryption TS packet from an inverter 4 is decoded using the key contained there, and MPEG decoding is further carried out. And the video data or audio data obtained as a result of the decoding is supplied to a monitor 3, and is outputted as a display or voice as an image, respectively.
[0026] Next, drawing 2 shows the example of a configuration of the digital CS tuner 2 of drawing 1 .
[0027] The input signal outputted when an antenna 1 receives a digital satellite broadcast wave is supplied to the front end section 12.
[0028] The front end section 12 performs the recovery of the input signal from an antenna 1 etc., obtains a transport stream, and supplies it to a descrambler 13. A descrambler 13 solves the scramble which lasts to the transport stream from the front end section 12, and supplies it to a switch 14. A switch 14 chooses the transport stream supplied from a descrambler 13, and outputs it to DEMUX (demultiplexer)15.

[0029] Under control of CPU21, from the transport stream supplied from a switch 14, DEMUX15 extracts TS packet of a predetermined channel, and supplies it to the AV decoder 16. The AV decoder 16 carries out MPEG (Moving Picture Experts Group) decoding of the TS packet from DEMUX15 under control of CPU21, and outputs the video data and audio data which are obtained as a result to the OSD (On Screen Display) processing section 17. In the OSD processing section 17, under control of CPU21, the video data from the AV decoder 16 is overlapped on a required predetermined image (for example, sound volume and the display of the channel chosen), and it is outputted to the D/A (Digtal/Analog) converter 18. By carrying out D/A conversion of the digital contents (here a video data and audio data) which the OSD processing section 17 outputs, D/A converter 18 considers as an analog signal, for example, is outputted to monitor 3 grade.
[0030] As for the digital contents broadcast as digital satellite broadcasting service as mentioned above, an indication etc. is given in a monitor 3.
[0031] On the other hand, in recording the digital contents broadcast as digital satellite broadcasting service, a switch 14 chooses the transport stream from a descrambler 13, and supplies it to a link (LINK Integrated Curcuit) IC 20. Under control of CPU21, a link IC 20 processes the link layer in the layer structure of an IEEE1394 serial bus, and also enciphers the transport stream from a switch 14 based on DTCP. Namely, a link IC 20 carries out the encryption TS packet of the key further by inserting in the location in front of the first TS packet enciphered by the key etc. (addition) by enciphering a transport stream using 8 bytes of key changed every about 30 seconds. And a link IC 20 arranges this encryption TS packet to an isochronous (Isochronous) packet, and supplies it to FAI (PHY IC) IC 19. FAI IC 19 carries out the isochronous transfer of the isochronous packet from a link IC 20 through an IEEE1394 serial bus at an inverter 4.
[0032] TS packet as digital contents broadcast as digital satellite broadcasting service as mentioned above is supplied to an inverter 4 through an IEEE1394 serial bus, and in an inverter 4, after processing of the conversion and others to a DIF block etc. is performed, it is supplied and recorded on DVCR5 through an IEEE1394 serial bus.
[0033] Next, when reproducing the digital contents recorded by DVCR5 as mentioned above, in DVCR5, the DIF block as the digital contents is reproduced, and an inverter 4 is supplied through an IEEE1394 serial bus. In an inverter 4, processing of the conversion and others to TS packet etc. is performed to the DIF block from DVCR5. Furthermore, the isochronous packet by which TS packet has been arranged consists of inverters 4, and an isochronous transfer is carried out through an IEEE1394 serial bus at the digital satellite tuner 2.
[0034] In the digital satellite tuner 2, in FAI IC 19, the isochronous packet by which TS packet (encryption TS packet) from an inverter 4 has been arranged is received, and a link IC 20 is supplied. A link IC 20 decodes the encryption TS packet arranged from FAI IC 19 to an isochronous packet under control of CPU21 using the key to which it is added there (contained), and supplies it to a switch 14. A switch 14 chooses TS packet from a link IC 20, and outputs it to DEMUX15, in DEMUX15, the AV decoder 16, the OSD processing section 17, and D/A converter 18, the same processing as the case where it mentions above is performed hereafter, and the image and voice as digital contents which were recorded by DVCR5 are outputted from a monitor 3.
[0035] In addition, the packet which received the link IC 20 from FAI IC 19 outputs the packet to a switch 14, when AV data (a video data, audio data) are arranged. Moreover, the packet which received the link IC 20 from FAI IC 19 outputs the packet to CPU21, when a command is arranged.
[0036] Moreover, CPU21 is performing the program memorized by memory 22, and it performs the transaction layer in the layer structure of an IEEE1394 serial bus, processing of serial bus management (Serial Bus Management), etc. while it controls DEMUX15, the AV decoder 16, and the OSD processing section 17.
[0037] Furthermore, memory 22 has memorized the program (firmware) for making control of DEMUX15, the AV decoder 16, and the OSD processing section 17, and processing of a transaction layer and serial bus management perform to CPU21. Moreover, memory 22 stores required data temporarily on actuation of CPU21.

[0038] Next, drawing 3 shows the example of a configuration of the inverter 4 of drawing 1 .
[0039] FAI IC 31 transmits and receives the data exchanged between the digital CS tuners 2 through an IEEE1394 serial bus. That is, FAI IC 31 transmits the packet from the MPEG link IC 32 to the digital CS tuner 2 through an IEEE1394 serial bus while it receives the packet transmitted from the digital CS tuner 2 through an IEEE1394 serial bus and supplies it to the MPEG link (MPEG-LINK-IC) IC 32.
[0040] The MPEG link IC 32 extracts the key (Key) added to the encryption TS packet, and supplies it to CPU35 while it supplies the encryption TS packet supplied from FAI IC 31 to the packet division section 33. Furthermore, the MPEG link IC 32 receives the key supplied from CPU35, is added to the original location of the encryption TS packet to which the key is supplied from the packet composition section 46 (insertion), and is supplied to FAI IC 31.
[0041] The packet division section 33 changes the encryption TS packet from the MPEG link IC 32 into a DIF block.
[0042] That is, in a format as it is, since TS packet is unrecordable by DVCR5, it is changed into a DIF block recordable by DVCR5 in the packet division section 33.
[0043] Specifically, a DIF block consists of 80 bytes, as shown in drawing 4 (A). And ID (Identification) for identifying a DIF block to 3 bytes of the head is arranged, and data are arranged at the remaining 77 bytes.
[0044] On the other hand, generally TS packet consists of 188 bytes. For this reason, as TS packet is divided and it is shown in drawing 4 (B), the packet division section 33 is dividing into three DIF blocks and arranging, and changes TS packet into a DIF block.
[0045] That is, as shown in drawing 4 (A), ID is arranged at 3 bytes of the head of three DIF blocks. Furthermore, after 3 bytes of ID, 13 bytes of 0 as dummy data is arranged for all three DIF blocks. And in three DIB blocks, 188 bytes of TS packet is divided into the remaining 64 bytes after dummy data, and it is arranged. However, with the gestalt of operation of drawing 4 , among three DIF blocks, although every 64 bytes of 188 bytes of TS packet (TRS) are arranged at the beginning and the 2nd DIF block, the time stump (TS (Time Stamp)) which are the remaining 60 bytes of 188 bytes of TS packet and 4 bytes which the cycle timer 43 mentioned later outputs is arranged at the last DIF block.
[0046] Return and a computing element 34 add the index supplied from CPU35 to a DIF block from the packet division section 33, and output it to a computing element 38 at drawing 3 . Namely, CPU35 receives the key added to the encryption TS packet supplied from the MPEG link IC 32. The index which can specify keys, such as the present time, is supplied to matching, and the index is supplied to a computing element 34. A computing element 34 The index which makes it such and is supplied from CPU35 is added to the DIF block with which the encryption TS packet to which the key matched with the index was added has been arranged. Therefore, according to the index added to the DIF block, it can recognize whether the key matched with which location of the sequence of the encryption TS packet which the MPEG link IC 32 outputs to the packet division section 33 by the index is arranged.
[0047] Here, a DIF block is transmitted to DV device of DVCR5 grade considering 150 blocks as one unit, as shown in drawing 5 , and 149 BUROTSU except a top DIF block (called a header section (Header section)) is recorded on one truck of a digital video tape among the DIF block of 150. The index matched with the key used for decoding the encryption TS packet arranged at the DIF block which constitutes a unit as shown in drawing 5 from a computing element 34 is arranged at the predetermined DIF block of the DIF block shown by V0 in drawing 5 .
[0048] Again, return and CPU35 perform various kinds of processings to drawing 3 by performing the program memorized in memory 36.
[0049] That is, to the key added to the encryption TS packet supplied from the MPEG link IC 32, an index is supplied to matching and CPU35 supplies the index to a computing element 34, as mentioned above. Furthermore, CPU35 makes a key memory 37 supply and memorize the group of the matched index and key. Moreover, CPU35 receives an index from the index extract section 45, reads the key matched with the index from a key memory 37, and supplies it to the MPEG link IC 32. Furthermore, CPU35 controls the FIFO (First In First Out) section 39 and the SD link (SD-LINK-IC) IC 40.
[0050] Memory 36 has memorized the program for making processing which was mentioned above to

CPU35 perform. Furthermore, memory 36 stores required data temporarily on actuation of CPU35. A key memory 37 stores temporarily the group of the index supplied from CPU35, and a key memory. In addition, at DTCP, since 8 bytes of key used for encryption/decode of TS packet is updated every about 30 seconds as mentioned above, whenever it performs record of 1 hour in DVCR5, by the key memory 37, the index matched with the keys for about 9800 bytes and those keys will be memorized.

[0051] A computing element 38 adds the time stump which a cycle timer 43 outputs to the DIF block which a computing element 34 outputs, and outputs it to the FIFO section 39.

[0052] The FIFO section 39 stores temporarily the DIF block which the SD link IC 40 outputs at the time of playback, stores temporarily input FIFO39A outputted to a comparator 44, and the DIF block which a computing element 38 outputs at the time of record, and consists of output FIFO39B outputted to the SD link IC 40.

[0053] Here, generally the data rate of a transport stream is 4Mbps (Bit Per Second). On the other hand, supposing DVCR5 is based on SD specification, the record rate is 25Mbps extent. Therefore, without carrying out especially the time amount five axis control of the DIF block which changed TS packet, by having recorded by DVCR5, many record sections of a digital video tape will be used, and recording efficiency is bad. So, in input FIFO39A or output FIFO39B, by storing a DIF block temporarily, the time-axis extension or time base compaction is performed, respectively, the difference between the data rate of a transport stream and the record rate of DVCR5 can be absorbed, and efficient record can be performed now in DVCR5 in an inverter 4.

[0054] In addition, although that time base compaction is performed in output FIFO39B by storing a DIF block temporarily at the time of record of a DIF block, the original time interval between TS packets is spoiled by this time base compaction. Therefore, although it is necessary to restore the spoiled time interval at the time of playback therefore, in a computing element 38, a time stump is added to a DIF block.

[0055] As mentioned above, the difference of the data rate of a transport stream and the record rate of DVCR is absorbed, and efficient record is performed, and the detail is indicated by JP,11-74796,A (Japanese Patent Application No. No. 231943 [nine to]) for which this applicant applied previously about the approach of reproducing normally the data recorded by making it such.

[0056] The SD link IC 40 reads the DIF block memorized by output FIFO39B of the FIFO section 39 under control of CPU35, arranges it to an isochronous packet, and is supplied to FAI (PHY-IC) IC 41. Moreover, the SD link IC 40 receives the isochronous packet supplied from FAI IC 41, and supplies the DIF block arranged there to input FIFO39A of the FIFO section 39. Furthermore, the SD link IC 40 supplies a 60Hz clock to the PLL (Phase Lock Loop) circuit 42.

[0057] FAI IC 41 receives the isochronous packet by which carries out the isochronous transfer of the isochronous packet from the SD link IC 40 through an IEEE1394 serial cable at DVCR5, and an isochronous transfer is carried out through an IEEE1394 serial bus from DVCR5, and supplies it to the SD link IC 40.

[0058] The PLL circuit 42 outputs a predetermined clock to a cycle timer 43 synchronizing with the clock from the SD link IC 40. A cycle timer 43 counts the clock from the PLL circuit 42, and supplies the counted value to a computing element 38 and a comparator 44 as a time stump.

[0059] The time stump added to the DIF block with which the comparator 44 is memorized by input FIFO39A, Compare the time stump which a cycle timer 43 outputs, and the DIF block with which the time stump which is in agreement with the output of a cycle timer 43 is added is read from input FIFO39A. As it outputs to the index extract section 45 and this mentioned above, the time interval between TS packets spoiled by time base compaction is restored.

[0060] The index extract section 45 outputs the DIF block to the packet composition section 46 while it extracts the index added to the DIF block from the comparator 44 and outputs it to CPU35.

[0061] TS packet which divided into three DIF blocks and has been arranged is returned by compounding the three DIF blocks, and the packet composition section 46 outputs it to the MPEG link IC 32, as shown in drawing 4 (B).

[0062] Next, with reference to the flow chart of drawing 6 , the processing performed when recording

digital contents by DVCR5 is explained in an inverter 4.
[0063] When digital contents were recorded by DVCR5, as it mentioned above, through an IEEE1394 serial bus, to an inverter 4, the isochronous packet by which the encryption TS packet has been arranged is transmitted, and the isochronous packet is received by FAI IC 31 from the digital CS tuner 2. FAI IC 31 outputs the isochronous packet which received to the MPEG link IC 32, and the MPEG link IC 32 will supply the encryption TS packet arranged at the isochronous packet to the packet division section 33 in step S1, if an isochronous packet is received.
[0064] In the packet division section 33, in step S1, as the encryption TS packet from the MPEG link IC 32 is divided and drawing 4 explained, it changes into three DIF blocks and outputs to a computing element 34.
[0065] And it progresses to step S2 and it is judged in CPU35 whether the key was added to the encryption TS packet divided into the DIF block which the packet division section 33 outputted. namely, as mentioned above, when the key is added to the encryption TS packet which received from FAI IC 31, the MPEG link IC 32 The key is extracted and CPU35 is supplied. CPU35 In step S2, it judges whether the key was added to the encryption TS packet divided into the DIF block which the packet division section 33 outputted by whether it was made such and the key has been supplied from the MPEG link IC 32.
[0066] In step S2, when judged with the key not being added to an encryption TS packet, a computing element 34 outputs the DIF block which changed the encryption TS packet to a computing element 38, skips step S3 and S4, and progresses to step S5.
[0067] Moreover, in step S2, when judged with the key being added to the encryption TS packet, it progresses to step S3, and CPU35 outputs an index to the key, i.e., the key supplied from the MPEG link IC 32, and outputs matching and its index to a computing element 34. A computing element 34 adds the index from CPU35 to a DIF block from the packet division section 33, and outputs it to a computing element 38.
[0068] And it progresses to step S4, and CPU35 makes a key memory 37 supply and memorize the group of the index outputted to the computing element 34, and the key matched with it, and progresses to step S5.
[0069] At step S5, in a computing element 38, the time stump which a cycle timer 43 outputs is added, and it progresses to step S6, and is outputted to the DIF block which a computing element 34 outputs at output FIFO39B of the FIFO section 39. In output FIFO39B, the DIF block from a computing element 38 is memorized. And according to control of CPU35, reading appearance of the DIF block memorized by output FIFO39B is carried out, and via the SD link IC 40 and FAI IC 41, through an IEEE1394 serial bus, it is supplied to DVCR5 and memorized.
[0070] After processing of step S6 progresses to step S7, when judged with it having been judged and transmitted whether the following encryption TS packet has been transmitted from the digital CS tuner 2 through an IEEE1394 serial bus, it is received by FAI IC 31 and the encryption TS packet is supplied to the packet division section 33 through the MPEG link IC 32. And the same processing is repeated by step S1 return and the following.
[0071] Moreover, in step S7, when the following encryption TS packet is judged [not having been transmitted from the digital CS tuner 2, and] through an IEEE1394 serial bus (i.e., when transmission of the encryption TS packet for record is completed), processing is ended.
[0072] As mentioned above, in the inverter 4 which suited the specification of DTCP, are contained in the encryption TS packet from the digital CS tuner 2. While extracting the key used for encryption and decode, and the key is matched with the index for specifying it and is memorized Change an encryption TS packet into a DIF block recordable by DVCR5, and the index matched with the key is added to the location where the key of the DIF block was contained. Since it was made to output to DVCR5 of the exterior, while protecting digital contents from an illegal copy, it is recordable by substandard DVCR5 of DTCP.
[0073] That is, also in the IEEE1394 serial bus which connects the digital CS tuner 2 and an inverter 4, also in the IEEE1394 serial bus which connects an inverter 4 and DVCR5, it is enciphered, therefore the

data to which that is transmitted can protect digital contents from an illegal copy. Furthermore, since the digital contents which the digital CS tuner 2 outputs are supplied to DVCR5 through the inverter 4 which suited the specification of DTCP, they can record the digital contents which the digital CS tuner 2 outputs in DVCR5 which does not conform to the specification of DTCP.

[0074] Next, the processing performed when reproducing the digital contents recorded by DVCR5 as mentioned above in an inverter 4 with reference to the flow chart of drawing 7 is explained.

[0075] Through an IEEE1394 serial bus, the DIF block reproduced by DVCR5 is transmitted to an inverter 4, and in FAI IC 41, the DIF block from DVCR5 is received and it is supplied to the SD link IC 40 with an inverter 4. The SD link IC 40 makes input 39A of the FIFO section 39 supply and memorize the DIF block from FAI IC 41 one by one.

[0076] And in step S11, a comparator 44 compares the time stump added to the oldest DIF block memorized by input FIFO39A with the time stump supplied from a cycle timer 43, and judges whether they are equal. In step S11, when judged with the time stump added to the DIF block and the time stump of a cycle timer 43 not being equal, it returns to step S11.

[0077] Moreover, when judged with the time stump added to the DIF block and the time stump of a cycle timer 43 being equal in step S11, it progresses to step S12, and a comparator 44 reads the DIF block with which the time stump is added, and the DIF block with which a part of other encryption TS packets where the part is arranged at the DIF block are arranged from input FIFO39A, and outputs them to the index extract section 45.

[0078] In step S13, when it judges whether the index is added to the DIF block from the comparator 44 and it is not added, the index extract section 45 outputs the DIF block to the packet composition section 46, skips steps S14 and S15, and progresses to step S16.

[0079] Moreover, in step S13, when judged with the index being added to the DIF block from a comparator 44, it progresses to step S14, and the index extract section 45 extracts the index added to the DIF block, outputs it to CPU35, and progresses to step S15.

[0080] At step S15, CPU35 reads the key matched with the index from the index extract section 35 from a key memory 37, and outputs it to the MPEG link IC 32.

[0081] And it progresses to step S16, and in the packet composition section 46, the DIF block from the index extract section 45 is compounded by the original encryption TS packet, and is outputted to the MPEG link IC 32.

[0082] When the encryption TS packet from the packet composition section 46 is outputted to FAI IC 31 when a key is not supplied from CPU35, and the key has been supplied from CPU35, the MPEG link IC 32 adds the key to an encryption TS packet from the packet composition section 46, and outputs it to it at FAI IC 31. Thereby, from FAI IC 31, at the time of record, the same encryption TS packet of a condition as the time of having been transmitted from the digital CS tuner 2 is transmitted to the digital CS tuner 2 through an IEEE1394 serial bus, and with the digital CS tuner 2, as the digital contents transmitted through an inverter 4 from DVCR5 mentioned above, they are displayed on a monitor 3.

[0083] After processing of step S16, it progresses to step S17 and it is judged whether the DIF block is still memorized by input FIFO39A. In step S17, when judged with the DIF block still being memorized by input FIFO39A, the same processing is repeated by step S11 return and the following.

[0084] Moreover, in step S17, when judged with the DIF block not being memorized by input FIFO39A, playback of DVCR5 is completed, and when all DIF blocks acquired by the playback are processed, processing is ended.

[0085] As mentioned above, while extracting an index from the DIF block reproduced by DVCR5 of the exterior in an inverter 4 Carry out format conversion of the DIF block to an encryption TS packet, and the key matched with the index is added to the location where the index with which the encryption TS packet after the conversion was extracted was contained. Since it was made to output to the external digital CS tuner 2, in the digital CS tuner 2, as it was able to mention above, the encryption TS packet can be decoded, and the image and voice as digital contents can be reproduced.

[0086] In addition, although it was made to process in an inverter 4 in an above-mentioned case, without decoding the encryption TS packet from the digital CS tuner 2, an encryption TS packet can also be

processed once it decodes. That is, in the MPEG link IC 32, an encryption TS packet performs conversion to a DIF block etc., after decoding it using the key contained in an encryption TS packet, and after it enciphers the DIF block in the SD link IC 40, it can be made to record on DVCR5. While protecting digital contents from an illegal copy also in this case, it is recordable by substandard DVCR5 of DTCP.

[0087] However, after decoding the DIF block enciphered from DVCR5 in the SD link IC 40 at the time of playback in this case, conversion to TS packet etc. is performed, and after enciphering using a key (encryption based on the specification of DTCP), it is necessary to make it output that TS packet to the digital CS tuner 2 in the MPEG link IC 32.

[0088] Moreover, in DTCP, 2-bit EMI (Encryption Mode Indicator) as copy control information for controlling a copy is specified. It expresses that digital contents belong to a copy free-lancer when EMI is 00B (B expresses that the value before that is a binary number) (Copy-freely), and when EMI is 01B, digital contents express that it is what (No-more-copies) cannot carry out the copy beyond it. Furthermore, it expresses that digital contents are what (Copy-one-generation) may be copied only once when EMI is 10B, and when EMI is 11B, digital contents express that it is what (Copy-never) the copy is forbidden.

[0089] By the SD link IC 40 of an inverter 4 (drawing 3), it is possible to restrict whether from the DIF block inputted there, above EMI is detected and a DIF block is outputted to DVCR5 of the exterior based on the EMI. That is, it is able to make it not to output a DIF block to DVCR5 it is [DVCR] substandard equipment of DTCP except when EMI is Copy-freely for example, etc.

[0090] Furthermore, it is possible to make the SD link IC 40 operate EMI in the range which is not contrary to the specification of DTCP. That is, when EMI is 10B showing Copy-one-generation and it outputs a DIF block to DVCR5 of the exterior for example, it is possible to change the EMI into 01B showing No-more-copies. In addition, actuation of EMI can be made to be carried out by them only when the digital contents inputted into the inverter 4 are outputted from terminals other than the inputted terminal.

[0091] Moreover, in addition to the equipment of the class (what is equipment?) of equipment connected with FAI IC 41 through an IEEE1394 serial bus in CPU35 in an inverter 4, the class beforehand set up as checked the manufacturer, or a manufacturer, it is able to make it not to output a DIF block. In this case, it becomes possible to prevent the output of a DIF block to the equipment manufactured for the purpose of the illegal copy.

[0092] Next, drawing 8 shows the example of a configuration of the gestalt of other operations of the digital satellite broadcasting service receiving system which applied this invention. In addition, about the case in drawing 1 , and the corresponding part, the same sign is attached among drawing. That is, the digital satellite broadcasting service receiving system of drawing 8 is constituted like the case [change to the digital CS tuner 2 and an inverter 4, and the digital CS tuner 51 is formed, and also] in drawing 1 .

[0093] The digital CS tuner 51 has the function which made the digital CS tuner 2 and inverter 4 of drawing 1 in one.

[0094] That is, drawing 9 shows the example of a configuration of the digital CS tuner 51 of drawing 8 . In addition, about the digital CS tuner 2 of drawing 2 , and the corresponding part, the same sign is attached among drawing. That is, the packet division section 61, the packet composition section 62, and a key memory 63 are newly formed, and also the digital CS tuner 51 of drawing 9 is fundamentally constituted similarly with the digital CS tuner 2 of drawing 2 .

[0095] Like the packet division section 33 of drawing 3 , the packet division section 61 carries out format conversion of the TS packet which a switch 14 outputs to a DIF block, and outputs it to a link IC 20. Like the packet composition section 46 of drawing 3 , the packet composition section 62 carries out format conversion of the DIF block which a link IC 20 outputs to the original TS packet, and supplies it to a switch 14. A key memory 63 memorizes the group of the key and index which are supplied from CPU21 like the key memory 37 of drawing 3 .

[0096] In addition, the program for operating the digital CS tuner 51 besides [which was explained by

drawing 2] a program as inverters 4 is also memorized by the memory 22 of drawing 9 , therefore CPU21 also performs processing to which an inverter 4 carries out in it.
[0097] In the digital CS tuner 51 constituted as mentioned above, an indication etc. is given for the digital contents broadcast as digital satellite broadcasting service to a monitor 3 like the case in drawing 2 .
[0098] On the other hand, when recording the digital contents broadcast as digital satellite broadcasting service, a switch 14 supplies the transport stream from a descrambler 13 to the packet division section 61, in the packet division section 61, format conversion of the TS packet which constitutes a transport stream is carried out to a DIF block, and it is supplied to a link IC 20.
[0099] By the link IC 20, TS packet divided into the DIF block is enciphered like the case in drawing 2 under control of CPU21 using the key which carries out time amount change. Furthermore, by the link IC 20, from the encryption result, a key is extracted and CPU21 is supplied. CPU21 makes an index memorize from a link IC 20 to a key to matching and a key memory 63. Furthermore, CPU21 supplies the index matched with the key to a link IC 20, and the index is added to a DIF block like the case in the computing element 34 of drawing 3 by the link IC 20. Then, by the link IC 20, addition of a time stump to a DIF block, time base compaction of a DIF block, etc. are performed under control of CPU21, and it is outputted to FAI IC 19. FAI IC 19 transmits the DIF block from a link IC 20 to DVCR5 through an IEEE1394 serial bus, and, thereby, the DIF block is recorded by DVCR5.
[0100] Next, if the DIF block recorded as mentioned above is reproduced by DVCR5, the reproduced DIF block will be transmitted to the digital CS tuner 51 through an IEEE1394 serial bus. In the digital CS tuner 51, in FAI IC 19, the DIF block from DVCR5 is received and a link IC 20 is supplied. By the link IC 20, time-axis extension of a DIF block etc. is performed and the index added to the DIF block is extracted after that. This index is supplied to CPU21 from a link IC 20, and if an index is received from a link IC 20, CPU21 will read the key matched with that index from a key memory 3, and will supply it to a link IC 20. By the link IC 20, TS packet currently divided into the DIF block is decoded using the key from CPU21, and it is outputted to the packet composition section 62.
[0101] In the packet composition section 62, the DIF block from a link IC 20 is compounded by the original TS packet, and is supplied to a switch 14. And in a switch 14, DEMUX15, the AV decoder 16, the OSD processing section 17, and D/A converter 18, the same processing as the case where it mentions above is performed hereafter, and, thereby, the image and voice as digital contents which were recorded by DVCR5 are outputted from a monitor 3.
[0102] Next, hardware can also perform a series of processings mentioned above, and software can also perform. When software performs a series of processings, the program which constitutes the software is installed in the computer (CPU35 of drawing 3 and CPU21 of drawing 9 correspond) built into the inverter 4 and the digital CS tuner 51 as hardware of dedication, a general-purpose computer, etc.
[0103] Then, the record medium which is used in order to install in a computer the program which performs a series of processings mentioned above and to make it into the condition which can be performed by computer with reference to drawing 10 and with which the program is recorded is explained.
[0104] A program is recordable on the hard disk 102 and semiconductor memory 103 as a record medium which are built in the computer 101 beforehand, as shown in drawing 10 (A).
[0105] Or a program is permanently [temporarily or] storable in record media, such as a floppy disk 111, CD-ROM (Compact Disc Read Only Memory)112, the MO (Magneto optical) disk 113, DVD (Digital Versatile Disc)114, a magnetic disk 115, and semiconductor memory 116, again, as shown in drawing 10 (B) (record). Such a record medium can be offered as the so-called software package.
[0106] In addition, it is installable in the hard disk 102 built [in / transmit to a computer 123 with a cable through the networks / **** / transmitting to a computer 101 on radio / 131 through / as it installs in a computer from a record medium which mentioned the program above and also is shown in drawing 10 (C) / the satellite 122 for the digital satellite broadcasting services from the download site 121, such as LAN (Local Area Network) and the Internet, and / a computer 101] in.
[0107] It is not necessary to necessarily process the processing step which describes the program for

making various kinds of processings perform to a computer in this description here to time series in accordance with the sequence indicated as a flow chart, and it is a juxtaposition thing also including the processing (for example, parallel processing or processing by the object) performed according to an individual.

[0108] Moreover, a program may be processed by the computer of 1 and distributed processing may be carried out by two or more computers. Furthermore, a program may be transmitted to a distant computer and may be executed.

[0109] Next, drawing 11 shows the example of a configuration of the computer 101 of drawing 10 .

[0110] The computer 101 contains CPU (Central Processing Unit)142, as shown in drawing 11 . The input/output interface 145 is connected to CPU142 through the bus 141, and CPU142 will perform the program stored in ROM (Read Only Memory)143 corresponding to the semiconductor memory 103 of drawing 10 (A) according to it, if a command is inputted when the input section 147 which consists of a keyboard, a mouse, etc. is operated by the user through an input/output interface 145. Or it is transmitted from the program and satellite 122 with which CPU142 is stored in the hard disk 102 again, or a network 131, and the program which reading appearance was carried out from the program which was received in the communications department 148 and installed on the hard disk 102 or the floppy disk 111 with which the drive 149 was equipped, CD-ROM112, MO disk 113, DVD114, or the magnetic disk 115, and was installed on the hard disk 102 is loaded to RAM (Random Access Memory)144, and is performed. And CPU142 outputs the processing result to the display 146 which consists of LCD (Liquid CryStal Display) etc. through an input/output interface 145 if needed.

[0111] In addition, although the gestalt of this operation explained the case where this invention was applied to the digital satellite broadcasting service receiving system which receives digital satellite broadcasting service, in addition to this, this invention is applicable to the equipment which deals with digital contents.

[0112] Moreover, the stream which is decoded by the principle same with decoding the TS packet besides the stream which consists of 188 bytes of TS packets, for example, consists of 130 bytes of packets which U.S. DirecTV uses by DSS (Direct Satellite System) is contained in the transport stream in this description.

[0113]

[Effect of the Invention] Like the above, according to the record medium to the data processor of this invention and the data-processing approach, and a list, the key contained in encryption data is extracted, and the key matches with the index for specifying it, and it memorizes. Furthermore, encryption data are changed into the data of a predetermined format, and the index matched with the key is added to the location where the key of the data of the predetermined format was contained, and it is outputted to it outside. On the other hand, an index is extracted and the data of the predetermined format are changed into the encryption data of the original format from the data of the predetermined format supplied from the outside. And the key matched with the index is added to the location where the index of encryption data was contained, and it is outputted to it outside. Therefore, digital contents can be protected from an illegal copy and record and playback can be performed in the form of a predetermined format.

[Translation done.]

* NOTICES *

JPO and INPIT are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] A key extract means to be the data processor which processes the encryption data which are data enciphered using the predetermined key, and to extract said key contained in said encryption data, A storage means to match said key with the index for specifying it, and to memorize it, The 1st format conversion means which changes said encryption data into the data of a predetermined format, An index addition means to add the index matched with the key to the location where said key of the data of said predetermined format was contained, The 1st output means which outputs outside the data of said predetermined format with which said index was added, An index extract means to extract said index from the data of said predetermined format supplied from the outside, The 2nd format conversion means which changes the data of said predetermined format into said encryption data of the original format, The data processor characterized by including a key addition means to add said key matched with the index to the location where said index of said encryption data was contained, and the 2nd output means which outputs outside said encryption data with which said key was added.
[Claim 2] Said encryption data are a data processor according to claim 1 characterized by being a transport stream.
[Claim 3] The data of said predetermined format are a data processor according to claim 1 characterized by being data of a DIF (Digital Interface) format.
[Claim 4] Said 1st output means is a data processor according to claim 1 characterized by restricting the output of the data of a format predetermined [said] with the specification of the equipment which receives the data of said predetermined format by which said encryption data were connected to whether a copy is permitted and or not the exterior.
[Claim 5] Said 1st output means is a data processor according to claim 1 characterized by operating the copy control information for controlling the copy about the data when outputting the data of said predetermined format.
[Claim 6] The key extract step which is the data-processing approach of processing the encryption data which are data enciphered using the predetermined key, and extracts said key contained in said encryption data, The storage step which matches said key with the index for specifying it, and memorizes it, The 1st format conversion step which changes said encryption data into the data of a predetermined format, The index addition step which adds the index matched with the key to the location where said key of the data of said predetermined format was contained, The 1st output step which outputs outside the data of said predetermined format with which said index was added, The index extract step which extracts said index from the data of said predetermined format supplied from the outside, The 2nd format conversion step which changes the data of said predetermined format into said encryption data of the original format, The data-processing approach characterized by including the key addition step which adds said key matched with the index to the location where said index of said encryption data was contained, and the 2nd output step which outputs outside said encryption data with which said key was added.
[Claim 7] The key extract step which is the record medium with which the program for making a

computer process the encryption data which are data enciphered using the predetermined key is recorded, and extracts said key contained in said encryption data, The storage step which matches said key with the index for specifying it, and memorizes it, The 1st format conversion step which changes said encryption data into the data of a predetermined format, The index addition step which adds the index matched with the key to the location where said key of the data of said predetermined format was contained, The 1st output step which outputs outside the data of said predetermined format with which said index was added, The index extract step which extracts said index from the data of said predetermined format supplied from the outside, The 2nd format conversion step which changes the data of said predetermined format into said encryption data of the original format, The key addition step which adds said key matched with the index to the location where said index of said encryption data was contained, The record medium characterized by recording the program containing the 2nd output step which outputs outside said encryption data with which said key was added.

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－94552
（P2001－94552A）
(43)公開日　平成13年４月６日(2001.4.6)

(51)Int.Cl.'	識別記号	ＦＩ	テーマコード'(参考)
Ｈ０４Ｌ　9/18		Ｇ０６Ｆ　12/14	３２０Ｂ　５Ｂ０１７
Ｇ０６Ｆ　12/14	３２０	Ｈ０４Ｌ　9/00	６５１　５Ｊ１０４
Ｈ０４Ｌ　9/08			６０１Ｃ

審査請求　未請求　請求項の数７　ＯＬ　（全 16 頁）

(21)出願番号　特願平11－267262

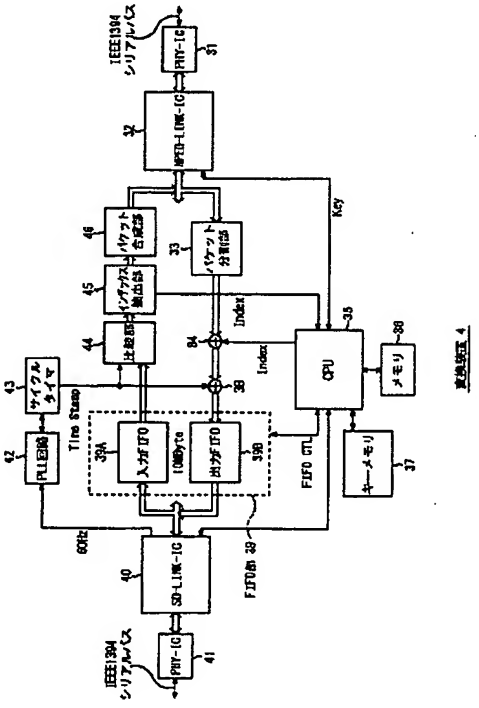
(22)出願日　平成11年９月21日(1999.9.21)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　森永　剛男
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100082131
弁理士　稲本　義雄

Ｆターム(参考)　5B017 AA06 BA07 BB02 BB03 CA06
CA16
5J104 AA12 AA16 EA02 EA15 JA04
NA02 NA32 PA05

(54)【発明の名称】　データ処理装置およびデータ処理方法、並びに記録媒体

(57)【要約】
【課題】　ディジタルコンテンツを違法なコピーから保護するとともに、ＤＴＣＰ(Digital Transmission Content Protection)の規格外のＤＶＣＲで記録する。
【解決手段】　ＤＴＣＰの規格に適合した変換装置４では、ＭＰＥＧリンクＩＣ３２において、ディジタルＣＳチューナからの暗号化ＴＳパケットに含まれている、暗号化および復号に用いるキーが抽出され、ＣＰＵ３５は、そのキーを、それを特定するためのインデックスと対応付けて、キーメモリ３７に記憶させる。また、パケット分割部３３では、暗号化ＴＳパケットが、ＤＶＣＲで記録可能なＤＩＦブロックに変換され、演算器３４では、そのＤＩＦブロックの、キーが含まれていた位置に、そのキーに対応付けられたインデックスが付加される。そして、その結果得られるＤＩＦブロックが、外部のＤＶＣＲに出力されて記録される。



1

【特許請求の範囲】

【請求項１】　所定のキーを用いて暗号化されたデータである暗号化データを処理するデータ処理装置であって、

前記暗号化データに含まれている前記キーを抽出するキー抽出手段と、

前記キーを、それを特定するためのインデックスと対応付けて記憶する記憶手段と、

前記暗号化データを、所定フォーマットのデータに変換する第１のフォーマット変換手段と、

前記所定フォーマットのデータの、前記キーが含まれていた位置に、そのキーに対応付けられたインデックスを付加するインデックス付加手段と、

前記インデックスが付加された前記所定フォーマットのデータを、外部に出力する第１の出力手段と、

外部から供給される前記所定フォーマットのデータから、前記インデックスを抽出するインデックス抽出手段と、

前記所定フォーマットのデータを、元のフォーマットの前記暗号化データに変換する第２のフォーマット変換手段と、

前記暗号化データの、前記インデックスが含まれていた位置に、そのインデックスに対応付けられた前記キーを付加するキー付加手段と、

前記キーが付加された前記暗号化データを、外部に出力する第２の出力手段とを含むことを特徴とするデータ処理装置。

【請求項２】　前記暗号化データは、トランスポートストリームであることを特徴とする請求項１に記載のデータ処理装置。

【請求項３】　前記所定フォーマットのデータは、ＤＩＦ(Digital Interface)フォーマットのデータであることを特徴とする請求項１に記載のデータ処理装置。

【請求項４】　前記第１の出力手段は、前記暗号化データがコピーが許可されたものであるかどうか、または外部に接続された前記所定フォーマットのデータを受信する装置の仕様によって、前記所定のフォーマットのデータの出力を制限することを特徴とする請求項１に記載のデータ処理装置。

【請求項５】　前記第１の出力手段は、前記所定フォーマットのデータを出力するときに、そのデータについてのコピーを制御するためのコピー制御情報を操作することを特徴とする請求項１に記載のデータ処理装置。

【請求項６】　所定のキーを用いて暗号化されたデータである暗号化データを処理するデータ処理方法であって、

前記暗号化データに含まれている前記キーを抽出するキー抽出ステップと、

前記キーを、それを特定するためのインデックスと対応付けて記憶する記憶ステップと、

2

前記暗号化データを、所定フォーマットのデータに変換する第１のフォーマット変換ステップと、

前記所定フォーマットのデータの、前記キーが含まれていた位置に、そのキーに対応付けられたインデックスを付加するインデックス付加ステップと、

前記インデックスが付加された前記所定フォーマットのデータを、外部に出力する第１の出力ステップと、

外部から供給される前記所定フォーマットのデータから、前記インデックスを抽出するインデックス抽出ステップと、

前記所定フォーマットのデータを、元のフォーマットの前記暗号化データに変換する第２のフォーマット変換ステップと、

前記暗号化データの、前記インデックスが含まれていた位置に、そのインデックスに対応付けられた前記キーを付加するキー付加ステップと、

前記キーが付加された前記暗号化データを、外部に出力する第２の出力ステップとを含むことを特徴とするデータ処理方法。

【請求項７】　所定のキーを用いて暗号化されたデータである暗号化データを、コンピュータに処理させるためのプログラムが記録されている記録媒体であって、

前記暗号化データに含まれている前記キーを抽出するキー抽出ステップと、

前記キーを、それを特定するためのインデックスと対応付けて記憶する記憶ステップと、

前記暗号化データを、所定フォーマットのデータに変換する第１のフォーマット変換ステップと、

前記所定フォーマットのデータの、前記キーが含まれていた位置に、そのキーに対応付けられたインデックスを付加するインデックス付加ステップと、

前記インデックスが付加された前記所定フォーマットのデータを、外部に出力する第１の出力ステップと、

外部から供給される前記所定フォーマットのデータから、前記インデックスを抽出するインデックス抽出ステップと、

前記所定フォーマットのデータを、元のフォーマットの前記暗号化データに変換する第２のフォーマット変換ステップと、

前記暗号化データの、前記インデックスが含まれていた位置に、そのインデックスに対応付けられた前記キーを付加するキー付加ステップと、

前記キーが付加された前記暗号化データを、外部に出力する第２の出力ステップとを含むプログラムが記録されていることを特徴とする記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、データ処理装置およびデータ処理方法、並びに記録媒体に関し、特に、IEEE1394シリアルバス等を介して、ディジタルコンテンツ

を伝送し、規格外の記録装置等でも、その記録を行うことができるようにするデータ処理装置およびデータ処理方法、並びに記録媒体に関する。

【０００２】

【従来の技術】例えば、シリアルバス規格の１つであるIEEE(Institute of Electrical and Electronics Engineers)1394規格による通信は、データのアイソクロナス(isochronous)転送を行うことができることから、画像や音声といったリアルタイムで再生する必要のあるディジタルデータの転送に適しており、さらに、近年におけるマルチメディア通信の要請もあって、大きく注目されている。

【０００３】ところで、ディジタルビデオデータやディジタルオーディオデータ等のディジタルコンテンツは、その画質や音質を劣化させることなく、何度もコピーすることができるため、その著作権者等を違法なコピーから保護する必要がある。

【０００４】そこで、本件出願人であるソニー株式会社を含む５社によって、IEEE1394シリアルバスを介して接続した装置どうしの間で、ディジタルコンテンツを伝送するときの、そのディジタルコンテンツを保護するための規格として、５ＣＤＴＣＰ(Five Company Digital Transmission Content Protection)（以下、適宜、ＤＴＣＰという）が定められた。

【０００５】ＤＴＣＰでは、コピーフリーでないディジタルコンテンツの伝送に先立って、受信側が、コピーを制御するためのコピー制御情報を正しく取り扱えるかどうかの認証を相互に行い、その後、送信側において、ディジタルコンテンツを暗号化して伝送し、受信側において、その暗号化されたディジタルコンテンツを復号するようになっている。

【０００６】ＤＴＣＰによるディジタルコンテンツの暗号化は、時間変化するキーを生成し、そのキーを用いて行われる。暗号化されたディジタルコンテンツは、その暗号化に用いたキーを含めて、IEEE1394シリアルバス上を伝送され、受信側では、その暗号化されたディジタルコンテンツが、そこに含まれるキーを用いて復号される。

【０００７】ここで、ＤＴＣＰによれば、正確には、キーの初期値と、ディジタルコンテンツの暗号化に用いるキーの変更タイミングを表すフラグとが、暗号化されたディジタルコンテンツ（以下、適宜、暗号化コンテンツという）に含められる。そして、受信側では、その暗号化コンテンツに含まれるキーの初期値を、やはり、その暗号化コンテンツに含まれるフラグのタイミングで変更していくことで、暗号化に用いられたキーが生成され、暗号化コンテンツが復号される。なお、本明細書中においては、暗号化コンテンツに、その復号を行うためのキーが含まれていると等価であると考えても差し支えないため、以下では、そのように考えるものとする。

【０００８】

【発明が解決しようとする課題】以上から、例えば、ディジタルＣＳ(Communication Satellite)チューナで受信したディジタルコンテンツを、IEEE1394シリアルバスを介して、コピー制御情報を正しく取り扱えない規格外のＤＶＣＲ(Digital Video Tape Recoder)等で記録することはできない。

【０００９】しかしながら、今後は、ディジタルＣＳチューナで受信したディジタルコンテンツを、IEEE1394シリアルバスを介して、ＤＶＣＲに伝送して録画するような利用形態に対するニーズが増加していくことが予想される。

【００１０】また、ディジタルＣＳチューナが出力する暗号化コンテンツを、ＤＶＣＲで、そのまま録画すれば、ディジタルコンテンツを違法なコピーから保護することができるが、録画した暗号化コンテンツを視聴することはできない。即ち、従来においては、ＤＶＣＲで記録した暗号化コンテンツを再生し、ディジタルＣＳチューナに入力して、その復号を行うのは困難であった。

【００１１】本発明は、このような状況に鑑みてなされたものであり、ディジタルコンテンツを違法なコピーから保護するとともに、規格外のＤＶＣＲ等で記録すること等ができるようにするものである。

【００１２】

【課題を解決するための手段】本発明のデータ処理装置は、暗号化データに含まれているキーを抽出するキー抽出手段と、キーを、それを特定するためのインデックスと対応付けて記憶する記憶手段と、暗号化データを、所定フォーマットのデータに変換する第１のフォーマット変換手段と、所定フォーマットのデータの、キーが含まれていた位置に、そのキーに対応付けられたインデックスを付加するインデックス付加手段と、インデックスが付加された所定フォーマットのデータを、外部に出力する第１の出力手段と、外部から供給される所定フォーマットのデータから、インデックスを抽出するインデックス抽出手段と、所定フォーマットのデータを、元のフォーマットの暗号化データに変換する第２のフォーマット変換手段と、暗号化データの、インデックスが含まれていた位置に、そのインデックスに対応付けられたキーを付加するキー付加手段と、キーが付加された暗号化データを、外部に出力する第２の出力手段とを含むことを特徴とする。

【００１３】暗号化データは、トランスポートストリームとすることができる。

【００１４】所定フォーマットのデータは、ＤＩＦ(Digital Interface)フォーマットのデータとすることができる。

【００１５】第１の出力手段には、暗号化データがコピーが許可されたものであるかどうか、または外部に接続された所定フォーマットのデータを受信する装置の仕様

によって、所定のフォーマットのデータの出力を制限させることができる。また、第１の出力手段には、所定フォーマットのデータを出力するときに、そのデータについてのコピーを制御するためのコピー制御情報を操作させることができる。

【００１６】本発明のデータ処理方法は、暗号化データに含まれているキーを抽出するキー抽出ステップと、キーを、それを特定するためのインデックスと対応付けて記憶する記憶ステップと、暗号化データを、所定フォーマットのデータに変換する第１のフォーマット変換ステップと、所定フォーマットのデータの、キーが含まれていた位置に、そのキーに対応付けられたインデックスを付加するインデックス付加ステップと、インデックスが付加された所定フォーマットのデータを、外部に出力する第１の出力ステップと、外部から供給される所定フォーマットのデータから、インデックスを抽出するインデックス抽出ステップと、所定フォーマットのデータを、元のフォーマットの暗号化データに変換する第２のフォーマット変換ステップと、暗号化データの、インデックスが含まれていた位置に、そのインデックスに対応付けられたキーを付加するキー付加ステップと、キーが付加された暗号化データを、外部に出力する第２の出力ステップとを含むことを特徴とする。

【００１７】本発明の記録媒体は、暗号化データに含まれているキーを抽出するキー抽出ステップと、キーを、それを特定するためのインデックスと対応付けて記憶する記憶ステップと、暗号化データを、所定フォーマットのデータに変換する第１のフォーマット変換ステップと、所定フォーマットのデータの、キーが含まれていた位置に、そのキーに対応付けられたインデックスを付加するインデックス付加ステップと、インデックスが付加された所定フォーマットのデータを、外部に出力する第１の出力ステップと、外部から供給される所定フォーマットのデータから、インデックスを抽出するインデックス抽出ステップと、所定フォーマットのデータを、元のフォーマットの暗号化データに変換する第２のフォーマット変換ステップと、暗号化データの、インデックスが含まれていた位置に、そのインデックスに対応付けられたキーを付加するキー付加ステップと、キーが付加された暗号化データを、外部に出力する第２の出力ステップとを含むプログラムが記録されていることを特徴とする。

【００１８】本発明のデータ処理装置およびデータ処理方法、並びに記録媒体においては、暗号化データに含まれているキーが抽出され、そのキーが、それを特定するためのインデックスと対応付けて記憶される。さらに、暗号化データが、所定フォーマットのデータに変換され、その所定フォーマットのデータの、キーが含まれていた位置に、そのキーに対応付けられたインデックスが付加されて、外部に出力される。一方、外部から供給される所定フォーマットのデータから、インデックスが抽出され、その所定フォーマットのデータが、元のフォーマットの暗号化データに変換される。そして、暗号化データの、インデックスが含まれていた位置に、そのインデックスに対応付けられたキーが付加されて、外部に出力される。

【００１９】

【発明の実施の形態】図１は、本発明を適用したディジタル衛星放送受信システムの一実施の形態の構成例を示している。

【００２０】図示せぬディジタル衛星放送局から放送されてくるディジタル衛星放送波は、アンテナ１で受信され、ディジタルＣＳチューナ２に供給される。ディジタルＣＳチューナ２は、ＤＴＣＰに準拠した仕様を有し、アンテナ１から供給される信号から、所定の周波数帯域の受信信号を検波、復調し、ＭＰＥＧ(Moving Picture Experts Group)トランスポートストリームとする。さらに、ディジタルＣＳチューナ２では、そのトランスポートストリームを構成するＴＳパケット（Transport Stream パケット）のうち、所定の１つのチャンネルのものが抽出され、その抽出されたＴＳパケットに含まれる、ＭＰＥＧ２エンコードされたビデオデータやオーディオデータが、ＭＰＥＧ２デコードされる。そして、そのデコードの結果得られたビデオデータまたはオーディオデータは、モニタ３に供給され、それぞれ画像として表示または音声として出力される。

【００２１】また、ディジタルＣＳチューナ２では、トランスポートストリームから、１チャンネル以上のＴＳパケットが抽出され、ＤＴＣＰに準拠した方式で暗号化される。そして、その暗号化されたＴＳパケット（以下、適宜、暗号化ＴＳパケット）は、IEEE1394シリアルバスを介して、変換装置４に供給される。

【００２２】ここで、変換装置４は、IEEE1394シリアルバスを介して、ディジタルＣＳチューナ２との間で、ディジタルコンテンツのやりとりをする場合、ＤＴＣＰに準拠した通信を行うようになっている。従って、ディジタルＣＳチューナ２および変換装置４は、いずれも、相互認証を行った後、時間変化するキーを用いて、ディジタルコンテンツを暗号化し、その結果得られる暗号化コンテンツに、暗号化に用いたキーを含めて、IEEE1394シリアルバス上に出力するようになっている。

【００２３】変換装置４では、ディジタルＣＳチューナ２からの暗号化ＴＳパケットが、ＳＤ(Standard density)規格のＤＩＦ(Digital Interface)ブロックにフォーマット変換され、IEEE1394シリアルバスを介して、ＤＶＣＲ５に供給される。ＤＶ(Digital Video)機器であるＤＶＣＲ５では、変換装置４からのＤＩＦブロックが、図示せぬディジタルビデオテープに記録される。

【００２４】ここで、ＤＩＦフォーマットについては、例えば、HD Digital VCR Conferenceにおいてまとめら

れたSpecification of Consumer Use Digital VCRs等に、その詳細が記載されている。

【００２５】さらに、ＤＶＣＲ５では、ディジタルビデオテープに記録されたＤＩＦブロックが再生され、IEEE1394シリアルバスを介して、変換装置４に供給される。変換装置４では、ＤＶＣＲ５からのＤＩＦブロックが、元の暗号化ＴＳパケットにフォーマット変換され、IEEE1394シリアルバスを介して、ディジタルＣＳチューナ２に供給される。ディジタルＣＳチューナ２では、変換装置４からの暗号化ＴＳパケットが、そこに含まれるキーを用いて復号され、さらにＭＰＥＧデコードされる。そして、そのデコードの結果得られたビデオデータまたはオーディオデータは、モニタ３に供給され、それぞれ画像として表示または音声として出力される。

【００２６】次に、図２は、図１のディジタルＣＳチューナ２の構成例を示している。

【００２７】アンテナ１がディジタル衛星放送波を受信することにより出力する受信信号は、フロントエンド部１２に供給されるようになっている。

【００２８】フロントエンド部１２は、アンテナ１からの受信信号の復調等を行い、トランスポートストリームを得て、デスクランブラ１３に供給する。デスクランブラ１３は、フロントエンド部１２からのトランスポートストリームにかけられているスクランブルを解き、スイッチ１４に供給する。スイッチ１４は、デスクランブラ１３から供給されるトランスポートストリームを選択し、ＤＥＭＵＸ（デマルチプレクサ）１５に出力する。

【００２９】ＤＥＭＵＸ１５は、ＣＰＵ２１の制御の下、スイッチ１４から供給されるトランスポートストリームから、所定のチャンネルのＴＳパケットを抽出し、ＡＶデコーダ１６に供給するようになっている。ＡＶデコーダ１６は、ＣＰＵ２１の制御の下、ＤＥＭＵＸ１５からのＴＳパケットを、ＭＰＥＧ(Moving Picture Experts Group)デコードし、その結果得られるビデオデータおよびオーディオデータを、ＯＳＤ(On Screen Display)処理部１７に出力する。ＯＳＤ処理部１７では、ＣＰＵ２１の制御の下、所定の必要な画像（例えば、音量や、選択されているチャンネル等の表示）が、ＡＶデコーダ１６からのビデオデータに重畳され、Ｄ／Ａ(Digital/Analog)コンバータ１８に出力される。Ｄ／Ａコンバータ１８は、ＯＳＤ処理部１７が出力するディジタルコンテンツ（ここでは、ビデオデータおよびオーディオデータ）をＤ／Ａ変換することにより、アナログ信号とし、例えば、モニタ３等に出力する。

【００３０】以上のようにして、ディジタル衛星放送として放送されてくるディジタルコンテンツは、モニタ３において表示等される。

【００３１】一方、ディジタル衛星放送として放送されてくるディジタルコンテンツを記録する場合には、スイッチ１４は、デスクランブラ１３からのトランスポートストリームを選択して、リンクＩＣ(LINK Integrated Curcuit)２０に供給する。リンクＩＣ２０は、ＣＰＵ２１の制御の下、IEEE1394シリアルバスのレイヤ構造におけるリンク層の処理を行う他、スイッチ１４からのトランスポートストリームを、ＤＴＣＰに準拠して暗号化する。即ち、リンクＩＣ２０は、トランスポートストリームを、約３０秒ごとに変更される８バイトのキーを用いて暗号化し、さらに、キーを、そのキーによって暗号化した最初のＴＳパケットの直前の位置等に挿入（付加）することにより、暗号化ＴＳパケットする。そして、リンクＩＣ２０は、この暗号化ＴＳパケットを、アイソクロナス(Isochronous)パケットに配置して、ファイＩＣ（PHY IC）１９に供給する。ファイＩＣ１９は、リンクＩＣ２０からのアイソクロナスパケットを、IEEE1394シリアルバスを介して、変換装置４に、アイソクロナス転送する。

【００３２】以上のようにして、ディジタル衛星放送として放送されてくるディジタルコンテンツとしてのＴＳパケットは、IEEE1394シリアルバスを介して、変換装置４に供給され、変換装置４において、ＤＩＦブロック等への変換その他の処理が施された後、IEEE1394シリアルバスを介して、ＤＶＣＲ５に供給されて記録される。

【００３３】次に、上述のようにしてＤＶＣＲ５で記録されたディジタルコンテンツを再生する場合においては、ＤＶＣＲ５では、そのディジタルコンテンツとしてのＤＩＦブロックが再生され、IEEE1394シリアルバスを介して、変換装置４に供給される。変換装置４では、ＤＶＣＲ５からのＤＩＦブロックに対して、ＴＳパケット等への変換その他の処理が施される。さらに、変換装置４では、ＴＳパケットが配置されたアイソクロナスパケットが構成され、IEEE1394シリアルバスを介して、ディジタル衛星チューナ２にアイソクロナス転送される。

【００３４】ディジタル衛星チューナ２では、ファイＩＣ１９において、変換装置４からのＴＳパケット（暗号化ＴＳパケット）が配置されたアイソクロナスパケットが受信され、リンクＩＣ２０に供給される。リンクＩＣ２０は、ＣＰＵ２１の制御の下、ファイＩＣ１９からのアイソクロナスパケットに配置された暗号化ＴＳパケットを、そこに付加されている（含まれている）キーを用いて復号し、スイッチ１４に供給する。スイッチ１４は、リンクＩＣ２０からのＴＳパケットを選択して、ＤＥＭＵＸ１５に出力し、以下、ＤＥＭＵＸ１５、ＡＶデコーダ１６、ＯＳＤ処理部１７、およびＤ／Ａコンバータ１８において、上述した場合と同様の処理が施され、ＤＶＣＲ５で記録されたディジタルコンテンツとしての画像および音声が、モニタ３から出力される。

【００３５】なお、リンクＩＣ２０は、ファイＩＣ１９から受信したパケットが、ＡＶデータ（ビデオデータ、オーディオデータ）が配置されたものである場合には、そのパケットを、スイッチ１４に出力する。また、リン

クＩＣ２０は、ファイＩＣ１９から受信したパケットが、コマンドが配置されたものである場合には、そのパケットを、ＣＰＵ２１に出力する。

【００３６】また、ＣＰＵ２１は、メモリ２２に記憶されたプログラムを実行することで、ＤＥＭＵＸ１５、ＡＶデコーダ１６、およびＯＳＤ処理部１７を制御するとともに、IEEE1394シリアルバスのレイヤ構造におけるトランザクション層やシリアルバス管理(Serial Bus Management)の処理等を行う。

【００３７】さらに、メモリ２２は、ＣＰＵ２１に、ＤＥＭＵＸ１５、ＡＶデコーダ１６、およびＯＳＤ処理部１７の制御や、トランザクション層およびシリアルバス管理の処理を行わせるためのプログラム（ファームウェア）を記憶している。また、メモリ２２は、ＣＰＵ２１の動作上必要なデータを、一時記憶するようにもなっている。

【００３８】次に、図３は、図１の変換装置４の構成例を示している。

【００３９】ファイＩＣ３１は、IEEE1394シリアルバスを介して、ディジタルＣＳチューナ２との間でやりとりされるデータの送受信を行うようになっている。即ち、ファイＩＣ３１は、IEEE1394シリアルバスを介して、ディジタルＣＳチューナ２から送信されてくるパケットを受信し、ＭＰＥＧリンクＩＣ(MPEG-LINK-IC)３２に供給するとともに、ＭＰＥＧリンクＩＣ３２からのパケットを、IEEE1394シリアルバスを介して、ディジタルＣＳチューナ２に送信するようになっている。

【００４０】ＭＰＥＧリンクＩＣ３２は、ファイＩＣ３１から供給される暗号化ＴＳパケットを、パケット分割部３３に供給するとともに、その暗号化ＴＳパケットに付加されているキー(Key)を抽出し、ＣＰＵ３５に供給するようになっている。さらに、ＭＰＥＧリンクＩＣ３２は、ＣＰＵ３５から供給されるキーを受信し、そのキーを、パケット合成部４６から供給される暗号化ＴＳパケットの、元の位置に付加（挿入）して、ファイＩＣ３１に供給するようになっている。

【００４１】パケット分割部３３は、ＭＰＥＧリンクＩＣ３２からの暗号化ＴＳパケットを、ＤＩＦブロックに変換するようになっている。

【００４２】即ち、ＴＳパケットは、そのままのフォーマットでは、ＤＶＣＲ５で記録することができないため、パケット分割部３３において、ＤＶＣＲ５で記録することのできるＤＩＦブロックに変換されるようになっている。

【００４３】具体的には、ＤＩＦブロックは、図４（Ａ）に示すように、８０バイトで構成される。そして、その先頭の３バイトには、ＤＩＦブロックを識別するためのＩＤ(Identification)が配置され、残りの７７バイトに、データが配置される。

【００４４】一方、ＴＳパケットは、一般に、１８８バイトで構成される。このため、パケット分割部３３は、ＴＳパケットを分割し、図４（Ｂ）に示すように、３つのＤＩＦブロックに分けて配置することで、ＴＳパケットをＤＩＦブロックに変換する。

【００４５】即ち、３つのＤＩＦブロックの先頭の３バイトには、図４（Ａ）に示したように、ＩＤが配置される。さらに、３つのＤＩＦブロックとも、３バイトのＩＤの後には、ダミーデータとしての１３バイトの０が配置される。そして、３つのＤＩＦブロックにおいて、ダミーデータの後の残りの６４バイトに、１８８バイトのＴＳパケットが分割されて配置される。但し、図４の実施の形態では、３つのＤＩＦブロックのうち、最初と２番目のＤＩＦブロックには、１８８バイトのＴＳパケット（ＴＲＳ）のうちの６４バイトずつが配置されるが、最後のＤＩＦブロックには、１８８バイトのＴＳパケットの残りの６０バイトと、後述するサイクルタイマ４３が出力する４バイトのタイムスタンプ（ＴＳ(Time Stamp)）とが配置される。

【００４６】図３に戻り、演算器３４は、パケット分割部３３からのＤＩＦブロックに、ＣＰＵ３５から供給されるインデックスを付加し、演算器３８に出力するようになっている。即ち、ＣＰＵ３５は、ＭＰＥＧリンクＩＣ３２から供給される、暗号化ＴＳパケットに付加されているキーに対して、現在の日時等の、キーを特定することのできるインデックスを対応付け、そのインデックスを、演算器３４に供給するようになっており、演算器３４は、そのようにしてＣＰＵ３５から供給されるインデックスを、そのインデックスに対応付けられたキーが付加されていた暗号化ＴＳパケットが配置されたＤＩＦブロックに付加するようになっている。従って、ＤＩＦブロックに付加されたインデックスによれば、ＭＰＥＧリンクＩＣ３２がパケット分割部３３に出力する暗号化ＴＳパケットのシーケンスのどの位置に、そのインデックスに対応付けられたキーが配置されていたかを認識することができる。

【００４７】ここで、ＤＩＦブロックは、図５に示すように、１５０ブロックを１つのユニットとして、ＤＶＣＲ５等のＤＶ機器に伝送され、その１５０のＤＩＦブロックのうち、先頭のＤＩＦブロック（ヘッダセクション(Header section)と呼ばれる）を除く１４９ブロッが、ディジタルビデオテープの１トラックに記録される。演算器３４では、図５に示すようなユニットを構成するＤＩＦブロックに配置された暗号化ＴＳパケットを復号するのに用いるキーに対応付けられたインデックスが、例えば、図５においてＶ０で示すＤＩＦブロック等の、所定のＤＩＦブロックに配置される。

【００４８】再び、図３に戻り、ＣＰＵ３５は、メモリ３６に記憶されたプログラムを実行することで、各種の処理を行うようになっている。

【００４９】即ち、ＣＰＵ３５は、上述したように、Ｍ

ＰＥＧリンクＩＣ３２から供給される、暗号化ＴＳパケットに付加されているキーに対して、インデックスを対応付け、そのインデックスを、演算器３４に供給する。さらに、ＣＰＵ３５は、その対応付けたインデックスとキーの組を、キーメモリ３７に供給して記憶させる。また、ＣＰＵ３５は、インデックス抽出部４５からインデックスを受信し、そのインデックスに対応付けられているキーを、キーメモリ３７から読み出して、ＭＰＥＧリンクＩＣ３２に供給する。さらに、ＣＰＵ３５は、FIFO(First In First Out)部３９およびＳＤリンクＩＣ(SD-LINK-IC)４０を制御する。

【００５０】メモリ３６は、ＣＰＵ３５に、上述したような処理を行わせるためのプログラムを記憶している。さらに、メモリ３６は、ＣＰＵ３５の動作上必要なデータを一時記憶するようにもなっている。キーメモリ３７は、ＣＰＵ３５から供給されるインデックスとキーメモリの組を一時記憶するようになっている。なお、ＤＴＣＰでは、上述したように、ＴＳパケットの暗号化／復号に用いられる８バイトのキーが、約３０秒ごとに更新されるため、ＤＶＣＲ５において１時間の記録を行うごとに、キーメモリ３７では、約９８００バイト分のキーと、それらのキーに対応付けられたインデックスが記憶されることになる。

【００５１】演算器３８は、サイクルタイマ４３が出力するタイムスタンプを、演算器３４が出力するＤＩＦブロックに付加し、FIFO部３９に出力するようになっている。

【００５２】FIFO部３９は、再生時に、ＳＤリンクＩＣ４０が出力するＤＩＦブロックを一時記憶し、比較部４４に出力する入力FIFO３９Ａと、記録時に、演算器３８が出力するＤＩＦブロックを一時記憶し、ＳＤリンクＩＣ４０に出力する出力FIFO３９Ｂとから構成されている。

【００５３】ここで、トランスポートストリームのデータレートは、一般に、４Ｍｂｐｓ(Bit Per Second)である。一方、ＤＶＣＲ５が、ＳＤ規格に準拠したものであるとすると、その記録レートは２５Ｍｂｐｓ程度である。従って、ＴＳパケットを変換したＤＩＦブロックを、特に時間軸制御することなく、ＤＶＣＲ５で記録したのでは、ディジタルビデオテープの多くの記録領域が使用されないこととなり、記録効率が悪い。そこで、変換装置４では、入力FIFO３９Ａまたは出力FIFO３９Ｂにおいて、ＤＩＦブロックを一時記憶することにより、その時間軸伸張または時間軸圧縮をそれぞれ行い、トランスポートストリームのデータレートと、ＤＶＣＲ５の記録レートとの間の差を吸収して、ＤＶＣＲ５において、効率の良い記録を行うことができるようになっている。

【００５４】なお、出力FIFO３９Ｂでは、ＤＩＦブロックの記録時に、ＤＩＦブロックが一時記憶されることにより、その時間軸圧縮が行われるが、この時間軸圧縮により、ＴＳパケット間の元の時間間隔が損なわれる。従って、再生時には、その損なわれた時間間隔を復元する必要があるが、そのために、演算器３８において、ＤＩＦブロックにタイムスタンプが付加される。

【００５５】以上のように、トランスポートストリームのデータレートと、ＤＶＣＲの記録レートとの差を吸収して、効率の良い記録を行い、かつそのようにして記録されたデータを正常に再生する方法については、本件出願人が先に出願した特開平１１－７４７９６号公報（特願平９－２３１９４３号）に、その詳細が開示されている。

【００５６】ＳＤリンクＩＣ４０は、ＣＰＵ３５の制御の下、FIFO部３９の出力FIFO３９Ｂに記憶されたＤＩＦブロックを読み出し、アイソクロナスパケットに配置して、ファイＩＣ(PHY-IC)４１に供給するようになっている。また、ＳＤリンクＩＣ４０は、ファイＩＣ４１から供給されるアイソクロナスパケットを受信し、そこに配置されているＤＩＦブロックをFIFO部３９の入力FIFO３９Ａに供給するようになっている。さらに、ＳＤリンクＩＣ４０は、例えば、６０Ｈｚのクロックを、ＰＬＬ(Phase Lock Loop)回路４２に供給するようにもなっている。

【００５７】ファイＩＣ４１は、ＳＤリンクＩＣ４０からのアイソクロナスパケットを、IEEE1394シリアルケーブルを介して、ＤＶＣＲ５に、アイソクロナス転送し、また、ＤＶＣＲ５から、IEEE1394シリアルバスを介してアイソクロナス転送されてくるアイソクロナスパケットを受信し、ＳＤリンクＩＣ４０に供給するようになっている。

【００５８】ＰＬＬ回路４２は、ＳＤリンクＩＣ４０からのクロックに同期して、サイクルタイマ４３に所定のクロックを出力するようになっている。サイクルタイマ４３は、ＰＬＬ回路４２からのクロックをカウントし、そのカウント値を、タイムスタンプとして、演算器３８および比較部４４に供給するようになっている。

【００５９】比較部４４は、入力FIFO３９Ａに記憶されているＤＩＦブロックに付加されているタイムスタンプと、サイクルタイマ４３が出力するタイムスタンプとを比較し、サイクルタイマ４３の出力と一致するタイムスタンプが付加されているＤＩＦブロックを、入力FIFO３９Ａから読み出して、インデックス抽出部４５に出力するようになっており、これにより、上述したように、時間軸圧縮によって損なわれたＴＳパケット間の時間間隔が復元されるようになっている。

【００６０】インデックス抽出部４５は、比較部４４からのＤＩＦブロックに付加されているインデックスを抽出し、ＣＰＵ３５に出力するとともに、そのＤＩＦブロックを、パケット合成部４６に出力するようになっている。

【００６１】パケット合成部４６は、図４（Ｂ）に示し

たように、３つのＤＩＦブロックに分割して配置されたＴＳパケットを、その３つのＤＩＦブロックを合成することで元に戻し、ＭＰＥＧリンクＩＣ３２に出力するようになっている。

【００６２】次に、図６のフローチャートを参照して、変換装置４において、ディジタルコンテンツをＤＶＣＲ５で記録するときに行われる処理について説明する。

【００６３】ディジタルコンテンツをＤＶＣＲ５で記録する場合においては、上述したように、ディジタルＣＳチューナ２から、IEEE1394シリアルバスを介し、変換装置４に対して、暗号化ＴＳパケットが配置されたアイソクロナスパケットが送信され、そのアイソクロナスパケットは、ファイＩＣ３１で受信される。ファイＩＣ３１は、受信したアイソクロナスパケットを、ＭＰＥＧリンクＩＣ３２に出力し、ＭＰＥＧリンクＩＣ３２は、アイソクロナスパケットを受信すると、ステップＳ１において、そのアイソクロナスパケットに配置された暗号化ＴＳパケットを、パケット分割部３３に供給する。

【００６４】パケット分割部３３では、ステップＳ１において、ＭＰＥＧリンクＩＣ３２からの暗号化ＴＳパケットを分割し、図４で説明したように、３つのＤＩＦブロックに変換して、演算器３４に出力する。

【００６５】そして、ステップＳ２に進み、ＣＰＵ３５において、パケット分割部３３が出力したＤＩＦブロックに分割された暗号化ＴＳパケットに、キーが付加されていたかどうかが判定される。即ち、ＭＰＥＧリンクＩＣ３２は、上述したように、ファイＩＣ３１から受信した暗号化ＴＳパケットに、キーが付加されている場合には、そのキーを抽出して、ＣＰＵ３５に供給するようになっており、ＣＰＵ３５は、ステップＳ２において、そのようにして、ＭＰＥＧリンクＩＣ３２からキーが供給されてきたかどうかによって、パケット分割部３３が出力したＤＩＦブロックに分割された暗号化ＴＳパケットに、キーが付加されていたかどうかを判定する。

【００６６】ステップＳ２において、暗号化ＴＳパケットに、キーが付加されていないと判定された場合、演算器３４は、その暗号化ＴＳパケットを変換したＤＩＦブロックを、演算器３８に出力し、ステップＳ３およびＳ４をスキップして、ステップＳ５に進む。

【００６７】また、ステップＳ２において、暗号化ＴＳパケットに、キーが付加されていると判定された場合、ステップＳ３に進み、ＣＰＵ３５は、そのキー、即ち、ＭＰＥＧリンクＩＣ３２から供給されるキーに、インデックスを対応付け、そのインデックスを、演算器３４に出力する。演算器３４は、ＣＰＵ３５からのインデックスを、パケット分割部３３からのＤＩＦブロックに付加し、演算器３８に出力する。

【００６８】そして、ステップＳ４に進み、ＣＰＵ３５は、演算器３４に出力したインデックスと、それに対応付けたキーとの組を、キーメモリ３７に供給して記憶させ、ステップＳ５に進む。

【００６９】ステップＳ５では、演算器３８において、演算器３４が出力するＤＩＦブロックに、サイクルタイマ４３が出力するタイムスタンプが付加され、ステップＳ６に進み、FIFO部３９の出力FIFO３９Ｂに出力される。出力FIFO３９Ｂでは、演算器３８からのＤＩＦブロックが記憶される。そして、出力FIFO３９Ｂに記憶されたＤＩＦブロックは、ＣＰＵ３５の制御にしたがって読み出され、ＳＤリンクＩＣ４０およびファイＩＣ４１を経由し、IEEE1394シリアルバスを介して、ＤＶＣＲ５に供給されて記憶される。

【００７０】ステップＳ６の処理後は、ステップＳ７に進み、次の暗号化ＴＳパケットが、IEEE1394シリアルバスを介して、ディジタルＣＳチューナ２から伝送されてきたかどうかが判定され、伝送されてきたと判定された場合、その暗号化ＴＳパケットは、ファイＩＣ３１で受信され、ＭＰＥＧリンクＩＣ３２を介して、パケット分割部３３に供給される。そして、ステップＳ１に戻り、以下、同様の処理が繰り返される。

【００７１】また、ステップＳ７において、次の暗号化ＴＳパケットが、IEEE1394シリアルバスを介して、ディジタルＣＳチューナ２から伝送されてきていないと判定された場合、即ち、記録対象の暗号化ＴＳパケットの伝送が終了した場合、処理を終了する。

【００７２】以上のように、ＤＴＣＰの規格に適合した変換装置４において、ディジタルＣＳチューナ２からの暗号化ＴＳパケットに含まれている、暗号化および復号に用いるキーを抽出し、そのキーを、それを特定するためのインデックスと対応付けて記憶する一方、暗号化ＴＳパケットを、ＤＶＣＲ５で記録可能なＤＩＦブロックに変換し、そのＤＩＦブロックの、キーが含まれていた位置に、そのキーに対応付けられたインデックスを付加して、外部のＤＶＣＲ５に出力するようにしたので、ディジタルコンテンツを違法なコピーから保護するとともに、ＤＴＣＰの規格外のＤＶＣＲ５で記録することができる。

【００７３】即ち、ディジタルＣＳチューナ２と変換装置４とを接続するIEEE1394シリアルバスにおいても、変換装置４とＤＶＣＲ５とを接続するIEEE1394シリアルバスにおいても、そこを転送されるデータは暗号化されており、従って、ディジタルコンテンツを違法なコピーから保護することができる。さらに、ディジタルＣＳチューナ２が出力するディジタルコンテンツは、ＤＴＣＰの規格に適合した変換装置４を介して、ＤＶＣＲ５に供給されるので、ＤＴＣＰの規格に適合していないＤＶＣＲ５において、ディジタルＣＳチューナ２が出力するディジタルコンテンツを記録することができる。

【００７４】次に、図７のフローチャートを参照して、変換装置４において、上述のようにして、ＤＶＣＲ５で記録されたディジタルコンテンツを再生するときに行わ

れる処理について説明する。

【００７５】ＤＶＣＲ５で再生されたＤＩＦブロックは、IEEE1394シリアルバスを介して、変換装置４に転送され、変換装置４では、ファイＩＣ４１において、ＤＶＣＲ５からのＤＩＦブロックが受信され、ＳＤリンクＩＣ４０に供給される。ＳＤリンクＩＣ４０は、ファイＩＣ４１からのＤＩＦブロックを、順次、FIFO部３９の入力３９Ａに供給して記憶させる。

【００７６】そして、ステップＳ１１において、比較部４４は、入力FIFO３９Ａに記憶されている、最も古いＤＩＦブロックに付加されているタイムスタンプと、サイクルタイマ４３から供給されるタイムスタンプとを比較し、それらが等しいかどうかを判定する。ステップＳ１１において、ＤＩＦブロックに付加されているタイムスタンプと、サイクルタイマ４３のタイムスタンプとが等しくないと判定された場合、ステップＳ１１に戻る。

【００７７】また、ステップＳ１１において、ＤＩＦブロックに付加されているタイムスタンプと、サイクルタイマ４３のタイムスタンプとが等しいと判定された場合、ステップＳ１２に進み、比較部４４は、そのタイムスタンプが付加されているＤＩＦブロックと、そのＤＩＦブロックに一部が配置されている暗号化ＴＳパケットの他の一部が配置されているＤＩＦブロックを、入力FIFO３９Ａから読み出し、インデックス抽出部４５に出力する。

【００７８】インデックス抽出部４５は、ステップＳ１３において、比較部４４からのＤＩＦブロックに、インデックスが付加されているかどうかを判定し、付加されていない場合、そのＤＩＦブロックを、パケット合成部４６に出力し、ステップＳ１４およびＳ１５をスキップして、ステップＳ１６に進む。

【００７９】また、ステップＳ１３において、比較部４４からのＤＩＦブロックに、インデックスが付加されていると判定された場合、ステップＳ１４に進み、インデックス抽出部４５は、そのＤＩＦブロックに付加されているインデックスを抽出し、ＣＰＵ３５に出力して、ステップＳ１５に進む。

【００８０】ステップＳ１５では、ＣＰＵ３５は、インデックス抽出部３５からのインデックスと対応付けられているキーを、キーメモリ３７から読み出し、ＭＰＥＧリンクＩＣ３２に出力する。

【００８１】そして、ステップＳ１６に進み、パケット合成部４６において、インデックス抽出部４５からのＤＩＦブロックが、元の暗号化ＴＳパケットに合成され、ＭＰＥＧリンクＩＣ３２に出力される。

【００８２】ＭＰＥＧリンクＩＣ３２は、ＣＰＵ３５からキーが供給されてこない場合には、パケット合成部４６からの暗号化ＴＳパケットを、ファイＩＣ３１に出力し、また、ＣＰＵ３５からキーが供給されてきた場合には、パケット合成部４６からの暗号化ＴＳパケットに、そのキーを付加して、ファイＩＣ３１に出力する。これにより、ファイＩＣ３１からは、記録時に、ディジタルＣＳチューナ２から転送されてきたときと同じ状態の暗号化ＴＳパケットが、IEEE1394シリアルバスを介して、ディジタルＣＳチューナ２に転送され、ディジタルＣＳチューナ２では、このようにして、ＤＶＣＲ５から変換装置４を介して転送されてくるディジタルコンテンツが、上述したようにしてモニタ３に表示される。

【００８３】ステップＳ１６の処理後は、ステップＳ１７に進み、入力FIFO３９Ａに、ＤＩＦブロックが、まだ記憶されているかどうかが判定される。ステップＳ１７において、入力FIFO３９Ａに、ＤＩＦブロックが、まだ記憶されていると判定された場合、ステップＳ１１に戻り、以下、同様の処理が繰り返される。

【００８４】また、ステップＳ１７において、入力FIFO３９Ａに、ＤＩＦブロックが記憶されていないと判定された場合、即ち、ＤＶＣＲ５の再生が終了し、その再生によって得られたＤＩＦブロックをすべて処理した場合、処理を終了する。

【００８５】以上のように、変換装置４において、外部のＤＶＣＲ５で再生されたＤＩＦブロックから、インデックスを抽出するとともに、そのＤＩＦブロックを、暗号化ＴＳパケットにフォーマット変換し、その変換後の暗号化ＴＳパケットの、抽出されたインデックスが含まれていた位置に、そのインデックスに対応付けられたキーを付加して、外部のディジタルＣＳチューナ２に出力するようにしたので、ディジタルＣＳチューナ２では、上述したようにして、その暗号化ＴＳパケットを復号し、ディジタルコンテンツとしての画像や音声を再生することができる。

【００８６】なお、上述の場合には、変換装置４において、ディジタルＣＳチューナ２からの暗号化ＴＳパケットを復号せずに処理するようにしたが、暗号化ＴＳパケットは、一旦復号してから処理することも可能である。即ち、暗号化ＴＳパケットは、ＭＰＥＧリンクＩＣ３２において、暗号化ＴＳパケットに含まれるキーを用いて復号してから、ＤＩＦブロックへの変換等を行い、ＳＤリンクＩＣ４０において、そのＤＩＦブロックを暗号化してから、ＤＶＣＲ５に記録するようにすることが可能である。この場合も、ディジタルコンテンツを違法なコピーから保護するとともに、ＤＴＣＰの規格外のＤＶＣＲ５で記録することができる。

【００８７】但し、この場合、再生時には、ＳＤリンクＩＣ４０において、ＤＶＣＲ５からの、暗号化されたＤＩＦブロックを復号してから、ＴＳパケットへの変換等を行い、ＭＰＥＧリンクＩＣ３２において、そのＴＳパケットを、キーを用いて暗号化（ＤＴＣＰの規格に準拠した暗号化）してから、ディジタルＣＳチューナ２に出力するようにする必要がある。

【００８８】また、ＤＴＣＰにおいては、コピーを制御

するためのコピー制御情報としての２ビットのＥＭＩ(Encryption Mode Indicator)が規定されている。ＥＭＩが００Ｂ（Ｂは、その前の値が２進数であることを表す）である場合は、ディジタルコンテンツがコピーフリーのもの(Copy-freely)であることを表し、ＥＭＩが０１Ｂである場合には、ディジタルコンテンツが、それ以上のコピーをすることができないもの(No-more-copies)であることを表す。さらに、ＥＭＩが１０Ｂである場合は、ディジタルコンテンツが、１度だけコピーして良いもの(Copy-one-generation)であることを表し、ＥＭＩが１１Ｂである場合には、ディジタルコンテンツが、コピーが禁止されているもの(Copy-never)であることを表す。

【００８９】変換装置４（図３）のＳＤリンクＩＣ４０では、そこに入力されるＤＩＦブロックから、上述のようなＥＭＩを検出し、そのＥＭＩに基づいて、ＤＩＦブロックを、外部のＤＶＣＲ５に出力するかどうかを制限するようにすることが可能である。即ち、例えば、ＥＭＩが、Copy-freelyである場合以外は、ＤＴＣＰの規格外の装置であるＤＶＣＲ５には、ＤＩＦブロックを出力しないようにすること等が可能である。

【００９０】さらに、ＳＤリンクＩＣ４０には、ＥＭＩを、ＤＴＣＰの規格に反しない範囲で操作させることが可能である。即ち、例えば、ＥＭＩが、Copy-one-generationを表す１０Ｂとなっている場合において、ＤＩＦブロックを、外部のＤＶＣＲ５に出力するときには、そのＥＭＩを、No-more-copiesを表す０１Ｂに変更することが可能である。なお、ＥＭＩの操作は、変換装置４に入力されたディジタルコンテンツが、その入力された端子以外の端子から出力される場合にのみ行うようにすることが可能である。

【００９１】また、変換装置４では、ＣＰＵ３５において、ファイＩＣ４１と、IEEE1394シリアルバスを介して接続される装置の種類（装置が何であるか）や、メーカを確認するようにして、あらかじめ設定された種類やメーカの装置以外には、ＤＩＦブロックを出力しないようにすることが可能である。この場合、違法コピーを目的として製作された装置へのＤＩＦブロックの出力を防止することが可能となる。

【００９２】次に、図８は、本発明を適用したディジタル衛星放送受信システムの他の実施の形態の構成例を示している。なお、図中、図１における場合と対応する部分については、同一の符号を付してある。即ち、図８のディジタル衛星放送受信システムは、ディジタルＣＳチューナ２および変換装置４に替えて、ディジタルＣＳチューナ５１が設けられている他は、図１における場合と同様に構成されている。

【００９３】ディジタルＣＳチューナ５１は、図１のディジタルＣＳチューナ２と変換装置４とを一体的にした機能を有している。

【００９４】即ち、図９は、図８のディジタルＣＳチューナ５１の構成例を示している。なお、図中、図２のディジタルＣＳチューナ２と対応する部分については、同一の符号を付してある。即ち、図９のディジタルＣＳチューナ５１は、パケット分割部６１、パケット合成部６２、およびキーメモリ６３が新たに設けられている他は、図２のディジタルＣＳチューナ２と基本的に同様に構成されている。

【００９５】パケット分割部６１は、図３のパケット分割部３３と同様に、スイッチ１４が出力するＴＳパケットを、ＤＩＦブロックにフォーマット変換し、リンクＩＣ２０に出力するようになっている。パケット合成部６２は、図３のパケット合成部４６と同様に、リンクＩＣ２０が出力するＤＩＦブロックを、元のＴＳパケットにフォーマット変換し、スイッチ１４に供給するようになっている。キーメモリ６３は、図３のキーメモリ３７と同様に、ＣＰＵ２１から供給されるキーとインデックスとの組を記憶するようになっている。

【００９６】なお、図９のメモリ２２には、図２で説明したようなプログラムの他、ディジタルＣＳチューナ５１を、変換装置４として機能させるためのプログラムも記憶されており、従って、ＣＰＵ２１は、変換装置４が行う処理も行うようになっている。

【００９７】以上のように構成されるディジタルＣＳチューナ５１では、図２における場合と同様にして、ディジタル衛星放送として放送されてくるディジタルコンテンツが、モニタ３に表示等される。

【００９８】一方、ディジタル衛星放送として放送されてくるディジタルコンテンツを記録する場合には、スイッチ１４は、デスクランブラ１３からのトランスポートストリームを、パケット分割部６１に供給し、パケット分割部６１では、トランスポートストリームを構成するＴＳパケットが、ＤＩＦブロックにフォーマット変換され、リンクＩＣ２０に供給される。

【００９９】リンクＩＣ２０では、ＣＰＵ２１の制御の下、ＤＩＦブロックに分割されたＴＳパケットが、図２における場合と同様にして、時間変化するキーを用いて暗号化される。さらに、リンクＩＣ２０では、その暗号化結果から、キーが抽出され、ＣＰＵ２１に供給される。ＣＰＵ２１は、リンクＩＣ２０からのキーに、インデックスを対応付け、キーメモリ６３に記憶させる。さらに、ＣＰＵ２１は、キーに対応付けたインデックスを、リンクＩＣ２０に供給し、リンクＩＣ２０では、そのインデックスが、図３の演算器３４における場合と同様にして、ＤＩＦブロックに付加される。その後、リンクＩＣ２０では、ＣＰＵ２１の制御の下、ＤＩＦブロックに対するタイムスタンプの付加や、ＤＩＦブロックの時間軸圧縮等が行われ、ファイＩＣ１９に出力される。ファイＩＣ１９は、リンクＩＣ２０からのＤＩＦブロックを、IEEE1394シリアルバスを介して、ＤＶＣＲ５に転

送し、これにより、ＤＶＣＲ５では、そのＤＩＦブロックが記録される。

【０１００】次に、上述のようにして記録されたＤＩＦブロックが、ＤＶＣＲ５で再生されると、その再生されたＤＩＦブロックは、IEEE1394シリアルバスを介して、ディジタルＣＳチューナ５１に転送される。ディジタルＣＳチューナ５１では、ファイＩＣ１９において、ＤＶＣＲ５からのＤＩＦブロックが受信され、リンクＩＣ２０に供給される。リンクＩＣ２０では、ＤＩＦブロックの時間軸伸張等が行われ、その後、ＤＩＦブロックに付加されているインデックスが抽出される。このインデックスは、リンクＩＣ２０からＣＰＵ２１に供給され、ＣＰＵ２１は、リンクＩＣ２０からインデックスを受信すると、そのインデックスに対応付けられているキーを、キーメモリ３から読み出し、リンクＩＣ２０に供給する。リンクＩＣ２０では、ＣＰＵ２１からのキーを用いて、ＤＩＦブロックに分割されているＴＳパケットが復号され、パケット合成部６２に出力される。

【０１０１】パケット合成部６２では、リンクＩＣ２０からのＤＩＦブロックが、元のＴＳパケットに合成され、スイッチ１４に供給される。そして、以下、スイッチ１４、ＤＥＭＵＸ１５、ＡＶデコーダ１６、ＯＳＤ処理部１７、およびＤ／Ａコンバータ１８において、上述した場合と同様の処理が施され、これにより、ＤＶＣＲ５で記録されたディジタルコンテンツとしての画像および音声が、モニタ３から出力される。

【０１０２】次に、上述した一連の処理は、ハードウェアにより行うこともできるし、ソフトウェアにより行うこともできる。一連の処理をソフトウェアによって行う場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアとしての変換装置４やディジタルＣＳチューナ５１に組み込まれているコンピュータ（図３のＣＰＵ３５や、図９のＣＰＵ２１が相当する）や、汎用のコンピュータ等にインストールされる。

【０１０３】そこで、図１０を参照して、上述した一連の処理を実行するプログラムをコンピュータにインストールし、コンピュータによって実行可能な状態とするために用いられる、そのプログラムが記録されている記録媒体について説明する。

【０１０４】プログラムは、図１０（Ａ）に示すように、コンピュータ１０１に内蔵されている記録媒体としてのハードディスク１０２や半導体メモリ１０３に予め記録しておくことができる。

【０１０５】あるいはまた、プログラムは、図１０（Ｂ）に示すように、フロッピーディスク１１１、CD-ROM(Compact Disc Read Only Memory)１１２，MO(Magneto optical)ディスク１１３，DVD(Digital Versatile Disc)１１４、磁気ディスク１１５、半導体メモリ１１６などの記録媒体に、一時的あるいは永続的に格納（記録）しておくことができる。このような記録媒体は、いわゆるパッケージソフトウエアとして提供することができる。

【０１０６】なお、プログラムは、上述したような記録媒体からコンピュータにインストールする他、図１０（Ｃ）に示すように、ダウンロードサイト１２１から、ディジタル衛星放送用の人工衛星１２２を介して、コンピュータ１０１に無線で転送したり、LAN(Local Area Network)、インターネットといったネットワーク１３１を介して、コンピュータ１２３に有線で転送し、コンピュータ１０１において、内蔵するハードディスク１０２などにインストールすることができる。

【０１０７】ここで、本明細書において、コンピュータに各種の処理を行わせるためのプログラムを記述する処理ステップは、必ずしもフローチャートとして記載された順序に沿って時系列に処理する必要はなく、並列的あるいは個別に実行される処理（例えば、並列処理あるいはオブジェクトによる処理）も含むものである。

【０１０８】また、プログラムは、１のコンピュータにより処理されるものであっても良いし、複数のコンピュータによって分散処理されるものであっても良い。さらに、プログラムは、遠方のコンピュータに転送されて実行されるものであっても良い。

【０１０９】次に、図１１は、図１０のコンピュータ１０１の構成例を示している。

【０１１０】コンピュータ１０１は、図１１に示すように、CPU(Central Processing Unit)１４２を内蔵している。CPU１４２には、バス１４１を介して、入出力インタフェース１４５が接続されており、CPU１４２は、入出力インタフェース１４５を介して、ユーザによって、キーボードやマウス等で構成される入力部１４７が操作されることにより指令が入力されると、それにしたがって、図１０（Ａ）の半導体メモリ１０３に対応するROM(Read Only Memory)１４３に格納されているプログラムを実行する。あるいは、また、CPU１４２は、ハードディスク１０２に格納されているプログラム、衛星１２２若しくはネットワーク１３１から転送され、通信部１４８で受信されてハードディスク１０２にインストールされたプログラム、またはドライブ１４９に装着されたフロッピディスク１１１、CD-ROM１１２、MOディスク１１３、DVD１１４、若しくは磁気ディスク１１５から読み出されてハードディスク１０２にインストールされたプログラムを、RAM(Random Access Memory)１４４にロードして実行する。そして、CPU１４２は、その処理結果を、例えば、入出力インタフェース１４５を介して、LCD(Liquid CryStal Display)等で構成される表示部１４６に、必要に応じて出力する。

【０１１１】なお、本実施の形態では、本発明を、ディジタル衛星放送を受信するディジタル衛星放送受信システムに適用した場合について説明したが、本発明は、その他、ディジタルコンテンツを取り扱う装置に適用可能

である。

【０１１２】また、本明細書中におけるトランスポートストリームには、１８８バイトのＴＳパケットで構成されるストリームの他、そのＴＳパケットをデコードするのと同様の原理でデコードされる、例えば、米国のDirecTV社がＤＳＳ(Direct Satellite System)で用いている１３０バイトのパケットで構成されるストリーム等も含まれる。

【０１１３】

【発明の効果】以上の如く、本発明のデータ処理装置およびデータ処理方法、並びに記録媒体によれば、暗号化データに含まれているキーが抽出され、そのキーが、それを特定するためのインデックスと対応付けて記憶される。さらに、暗号化データが、所定フォーマットのデータに変換され、その所定フォーマットのデータの、キーが含まれていた位置に、そのキーに対応付けられたインデックスが付加されて、外部に出力される。一方、外部から供給される所定フォーマットのデータから、インデックスが抽出され、その所定フォーマットのデータが、元のフォーマットの暗号化データに変換される。そして、暗号化データの、インデックスが含まれていた位置に、そのインデックスに対応付けられたキーが付加されて、外部に出力される。従って、ディジタルコンテンツを違法なコピーから保護して、所定フォーマットの形で記録、再生を行うことができる。

【図面の簡単な説明】

【図１】本発明を適用したディジタル衛星放送受信システムの一実施の形態の構成例を示すブロック図である。

【図２】図１のディジタルＣＳチューナ２の構成例を示すブロック図である。

【図３】図１の変換装置４の構成例を示すブロック図である。

【図４】図３のパケット分割部３３の処理を説明するための図である。

【図５】図３の演算器３４の処理を説明するための図である。

【図６】ＤＶＣＲ５で記録を行う場合の、図３の変換装置４の処理を説明するためのフローチャートである。

【図７】ＤＶＣＲ５で再生を行う場合の、図３の変換装置４の処理を説明するためのフローチャートである。

【図８】本発明を適用したディジタル衛星放送受信システムの他の実施の形態の構成例を示すブロック図である。

【図９】図８のディジタルＣＳチューナ５１の構成例を示すブロック図である。

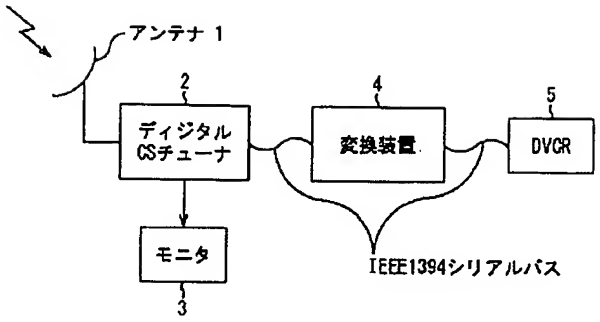
【図１０】本発明を適用した記録媒体を説明するための図である。

【図１１】図１０のコンピュータ１０１の構成例を示すブロック図である。

【符号の説明】

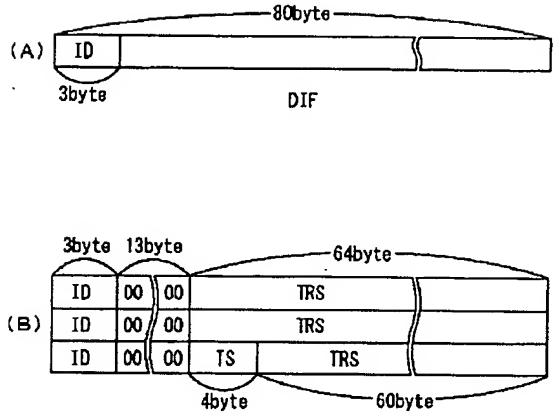
１ アンテナ，２ ディジタルＣＳチューナ，３ モニタ，４ 変換装置，５ ＤＶＣＲ，１２ フロントエンド部，１３ デスクランブラ，１４ スイッチ，１５ ＤＥＭＵＸ，１６ ＡＶデコーダ，１７ ＯＳＤ処理部，１８ Ｄ／Ａコンバータ，１９ ファイＩＣ，２０ リンクＩＣ，２１ ＣＰＵ，２２ メモリ，３１ ファイＩＣ，３２ ＭＰＥＧリンクＩＣ，３３ パケット分割部，３４ 演算器，３５ ＣＰＵ，３６メモリ，３７ キーメモリ，３８ 演算器，３９ FIFO部，３９Ａ入力FIFO，３９Ｂ 出力FIFO，４０ ＳＤリンクＩＣ，４１ ファイＩＣ，４２ ＰＬＬ回路，４３ サイクルタイマ，４４ 比較部，４５ インデックス抽出部，４６ パケット合成部，５１ ディジタルＣＳチューナ，６１ パケット分割部，６２ パケット合成部，６３ キーメモリ，１０１ コンピュータ，１０２ ハードディスク，１０３ 半導体メモリ，１１１ フロッピーディスク，１１２ CD-ROM，１１３ MOディスク，１１４ DVD，１１５ 磁気ディスク，１１６ 半導体メモリ，１２１ダウンロードサイト，１２２ 衛星，１３１ ネットワーク，１４１ バス，１４２ CPU，１４３ ROM，１４４ RAM，１４５ 入出力インタフェース，１４６ 表示部，１４７ 入力部，１４８ 通信部，１４９ドライブ

【図１】

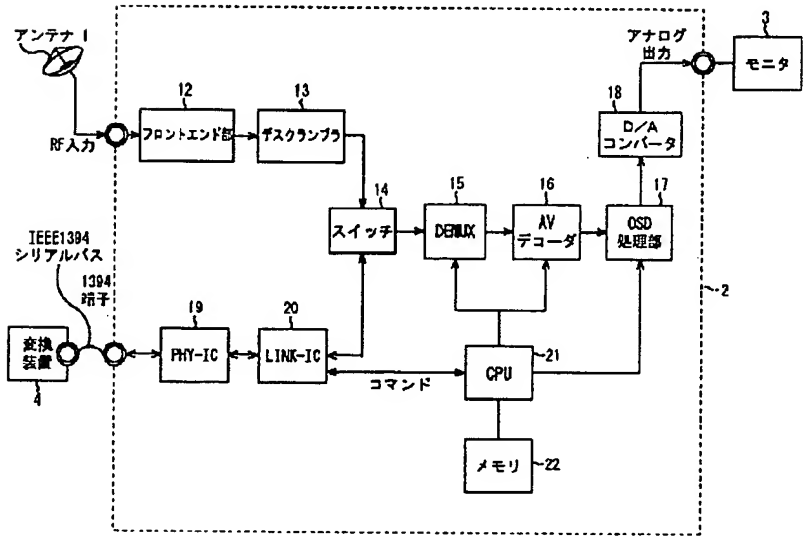


ディジタル衛星放送受信システム

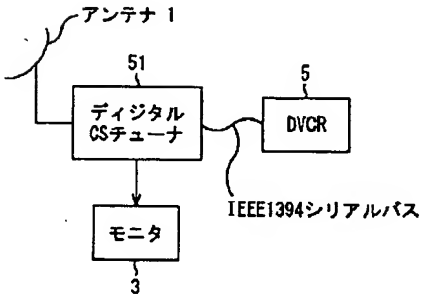
【図４】



【図２】

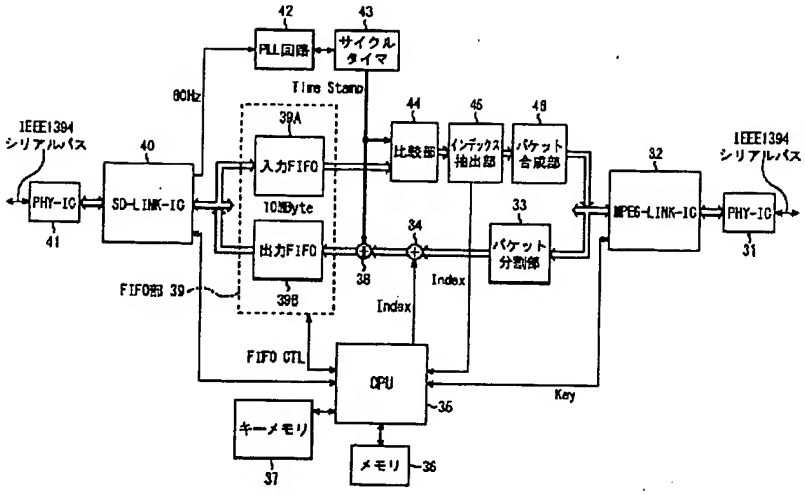


【図８】



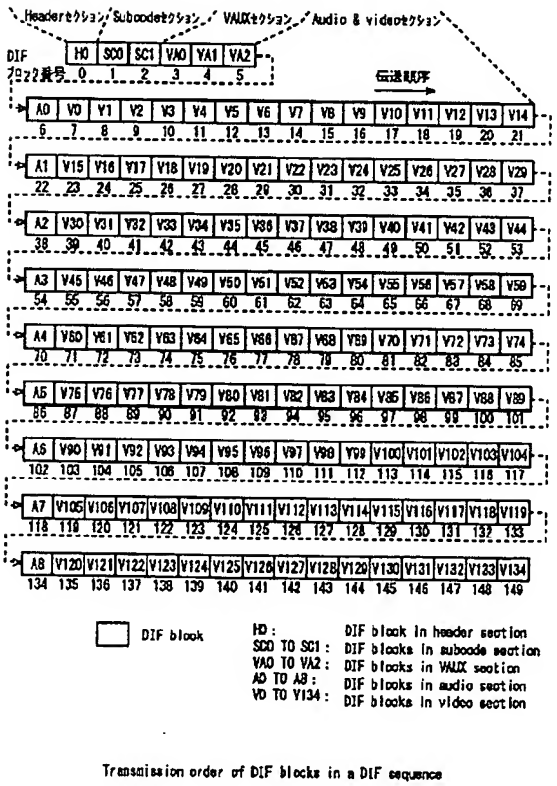
ディジタル衛星放送受信システム

【図3】



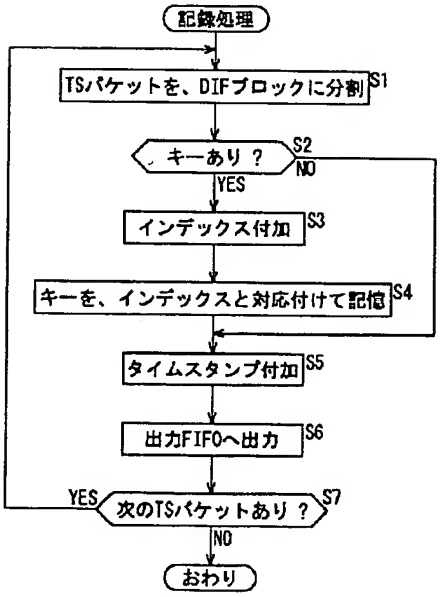
変換装置 4

【図5】

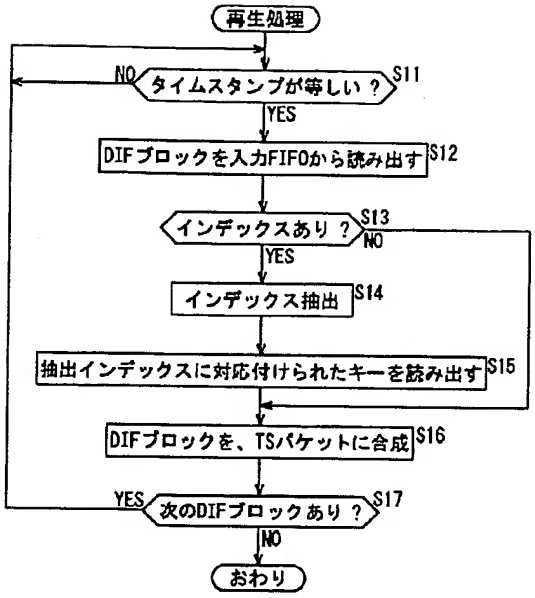


Transmission order of DIF blocks in a DIF sequence

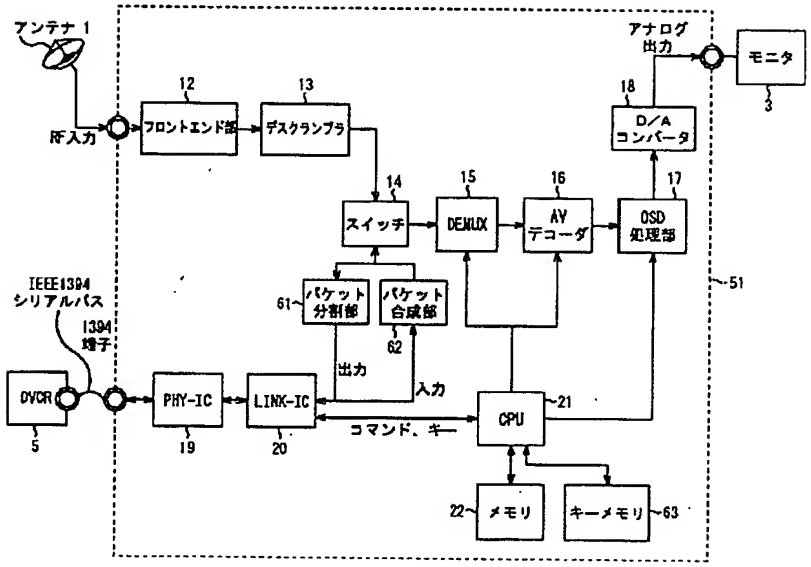
【図6】



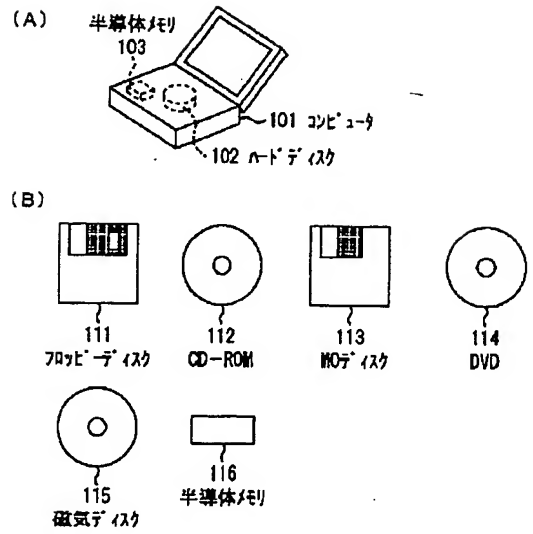
【図７】


再生処理
NO
タイムスタンプが等しい？
S11
YES
DIFブロックを入力FIFOから読み出す
S12
インデックスあり？
S13
NO
YES
インデックス抽出
S14
抽出インデックスに対応付けられたキーを読み出す
S15
DIFブロックを、TSパケットに合成
S16
YES
次のDIFブロックあり？
S17
NO
おわり

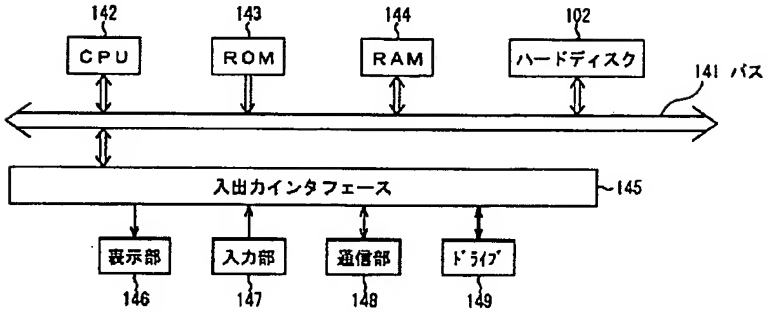
【図９】


アンテナ 1
RF入力
12
フロントエンド部
13
デスクランブラ
14
スイッチ
15
DEMUX
16
AV
デコーダ
17
OSD
処理部
18
D／A
コンバータ
アナログ
出力
モニタ
3
51
IEEE1394
シリアルバス
1394
端子
DVCR
5
PHY-IC
19
LINK-IC
20
61
パケット
分割部
パケット
合成部
62
出力
入力
コマンド、キー
CPU
21
22
メモリ
キーメモリ
63

【図10】



【図11】



コンピュータ 101

Family list
1 family member for: **JP2001094552**
Derived from 1 application

Back to JP2001094

1 **DEVICE AND METHOD FOR DATA PROCESSING AND RECORDING MEDIUM**

Inventor: MORINAGA TAKEO

Applicant: SONY CORP

EC:

IPC: ***G06F12/14; G06F21/24; H04L9/08*** (+10)

Publication info: JP2001094552 A - 2001-04-06

Data supplied from the ***esp@cenet*** database - Worldwide